ÜBER

ZERLEGUNGEN VON ZAHLEN

DURCH IHRE

GRÖSSTEN GEMEINSAMEN THEILER.

VON

R. DEDEKIND.

SONDER-ABDRUCK
AUS DER
„FESTSCHRIFT DER HERZOGL. TECHNISCHEN HOCHSCHULE CAROLO-WILHELMINA"
BEI
GELEGENHEIT DER 69. VERSAMMLUNG DEUTSCHER NATURFORSCHER
UND ÄRZTE IN BRAUNSCHWEIG.

BRAUNSCHWEIG,
DRUCK VON FRIEDRICH VIEWEG UND SOHN.
1897.

ÜBER

ZERLEGUNGEN VON ZAHLEN

DURCH IHRE

GRÖSSTEN GEMEINSAMEN THEILER.

VON

R. DEDEKIND.

Liegt ein endliches System von natürlichen Zahlen vor, und bildet man alle grössten gemeinsamen Theiler von zwei oder mehreren dieser Zahlen, so werden die letzteren hierdurch auf mannigfaltige Weise in Factoren zerlegt. Obgleich nun diese Factoren im Allgemeinen bekanntlich keine Primzahlen sind, so leisten sie doch für manche Untersuchungen ausreichende Dienste, und es verlohnt sich daher wohl der Mühe, die hierbei auftretenden Gesetze im Zusammenhange darzustellen. Dies ist der nächste Gegenstand des vorliegenden Aufsatzes, doch soll zugleich die ursprüngliche Aufgabe so viel wie möglich verallgemeinert und auch auf Gebiete übertragen werden, in denen es gar keine Zerlegungen in eigentliche Primfactoren giebt. Hierbei verliert zwar die Untersuchung ihr arithmetisches Gepräge fast ganz, so dass sie mathematische Kenntnisse kaum noch voraussetzt, aber zugleich treten die Gesetze und ihre Gründe deutlicher hervor, und ich darf hoffen, dass in dieser Hinsicht meine Arbeit doch einigen Mathematikern willkommen sein mag.

§. 1. Drei Zahlen.

Sind a, b, c drei gegebene natürliche Zahlen, so will ich den grössten gemeinsamen Theiler

$$\left.\begin{array}{llll} \text{der Zahlen } b, c & \text{mit } a_1 \\ \text{„ „ } c, a & \text{„ } b_1 \\ \text{„ „ } a, b & \text{„ } c_1 \\ \text{„ „ } a, b, c & \text{„ } d \end{array}\right\} \qquad (1)$$

bezeichnen; dann kann man, weil d offenbar auch der grösste gemeinsame Theiler von je zwei der drei Zahlen a_1, b_1, c_1 ist,

$$a_1 = d\,a', \quad b_1 = d\,b', \quad c_1 = d\,c' \qquad (2)$$

setzen, wo a', b', c' relative Primzahlen sind, womit in üblicher Weise ausgedrückt sein soll, dass je zwei äusserlich verschiedene dieser Zahlen, z. B. b', c', relative Primzahlen sind. Hieraus folgt, dass $d\,b'\,c'$ das kleinste gemeinsame Vielfache der Zahlen b_1, c_1 ist, und da a zufolge (1) durch beide theilbar ist, so erhält man die Zerlegungen

$$a = d\,b'\,c'\,a'', \quad b = d\,c'\,a'\,b'', \quad c = d\,a'\,b'\,c'' \qquad (3)$$

wo a'', b'', c'' ebenfalls natürliche Zahlen sind. Die drei gegebenen Zahlen a, b, c erscheinen daher als Producte von je vier der sieben

Zahlen d, a', b', c', a'', b'', c'', welche wir die *Kerne des Systems* a, b, c nennen wollen (vergl. §. 7). Zugleich ergiebt sich aus der Bedeutung von a_1, b_1, c_1, dass jedes der drei Paare

$$c'b'' \text{ und } b'c'', \quad a'c'' \text{ und } c'a'', \quad b'a'' \text{ und } a'b''$$

aus zwei relativen Primzahlen besteht; hierin liegt zunächst wieder, dass die drei Zahlen a', b', c' relative Primzahlen sind; dasselbe gilt offenbar von den drei Zahlen a'', b'', c'', und ausserdem besteht jedes der drei Paare

$$a' \text{ und } a'', \quad b' \text{ und } b'', \quad c' \text{ und } c''$$

aus zwei relativen Primzahlen, während die anderen Paare, wie a' und b'', diese Eigenschaft nicht zu besitzen brauchen. Ist z. B.

$$a = 420, \quad b = 800, \quad c = 216,$$

so findet man

$$\begin{aligned} a_1 &= 8, \quad b_1 = 12, \quad c_1 = 20, \quad d = 4, \\ a' &= 2, \quad b' = 3, \quad c' = 5, \\ a'' &= 7, \quad b'' = 20, \quad c'' = 9. \end{aligned}$$

Zufolge (2) und (3) lassen sich die sieben Kerne d, a', b', c', a'', b'', c'' durch die drei gegebenen Zahlen a, b, c und die aus ihnen gebildeten vier grössten gemeinsamen Theiler a_1, b_1, c_1, d in folgender Weise darstellen:

$$\left.\begin{aligned} d &= d \\ a' = \frac{a_1}{d}, \quad b' &= \frac{b_1}{d}, \quad c' = \frac{c_1}{d} \\ a'' = \frac{ad}{b_1 c_1}, \quad b'' &= \frac{bd}{c_1 a_1}, \quad c'' = \frac{cd}{a_1 b_1} \end{aligned}\right\} \tag{4}$$

Diese Kerne bleiben, mit Ausnahme von d, ungeändert, wenn man a, b, c durch drei beliebige, ihnen proportionale Zahlen ersetzt, welche auch *gebrochen* sein dürfen, falls man unter dem grössten gemeinsamen Theiler von rationalen Zahlen u, v, w ... immer diejenige positive rationale Zahl e versteht, für welche die Quotienten

$$\frac{u}{e}, \quad \frac{v}{e}, \quad \frac{w}{e} \ldots$$

ganze Zahlen ohne gemeinsamen Theiler werden [1]).

Ersetzt man aber die drei Zahlen a, b, c durch drei ihnen umgekehrt proportionale Zahlen, z. B. durch bc, ca, ab oder durch a^{-1}, b^{-1}, c^{-1}, so vertauscht sich a' mit a'', b' mit b'', c' mit c''; diese Erscheinung steht in unmittelbarem Zusammenhange mit dem Dualismus zwischen den Begriffen des grössten gemeinsamen Theilers und des kleinsten gemeinsamen Vielfachen [2]). Für jetzt mögen indessen fol-

[1]) Dirichlet's Vorlesungen über Zahlentheorie, 4. Aufl., §. 172, S. 515; dies Werk soll künftig mit D. citirt werden.

[2]) Vergl. D., §. 178, S. 555.

gende Bemerkungen genügen. Bezeichnet man das kleinste gemeinsame Vielfache

$$\left.\begin{array}{llll} \text{der Zahlen } b, c & \text{mit } a_2 \\ \text{„ „ } c, a & \text{„ } b_2 \\ \text{„ „ } a, b & \text{„ } c_2 \\ \text{„ „ } a, b, c & \text{„ } m \end{array}\right\} \quad (5)$$

so erhält man nach bekannten Regeln

$$\left.\begin{aligned} a_2 &= \frac{b\,c}{a_1} = d\,a'\,b'\,c'\,b''\,c'' \\ b_2 &= \frac{c\,a}{b_1} = d\,a'\,b'\,c'\,c''\,a'' \\ c_2 &= \frac{a\,b}{c_1} = d\,a'\,b'\,c'\,a''\,b'' \end{aligned}\right\} \quad (6)$$

Da ferner nach dem Obigen a'' relative Primzahl zu $a'\,b''\,c''$ ist, so haben die Zahlen a und a_2 zufolge (3) und (6) den grössten gemeinsamen Theiler $d\,b'\,c'$, und da m zufolge (5) ihr kleinstes gemeinsames Vielfaches, also $m\,.\,d\,b'\,c' = a\,a_2$ ist, so ergiebt sich

$$m = d\,a'\,b'\,c'\,a''\,b''\,c'' = \frac{a\,b\,c\,d}{a_1\,b_1\,c_1} \quad (7)$$

§. 2. Vier Zahlen.

Hat man mehr als drei gegebene Zahlen zu betrachten, so wird eine andere Bezeichnungsweise zweckmässig, deren Gebrauch jetzt erörtert werden soll. Die gegebenen Zahlen seien

$$(1,0),\ (2,0),\ (3,0),\ (4,0)\ \ldots, \quad (1)$$

und man bezeichne den grössten gemeinsamen Theiler

$$\left.\begin{array}{l} \text{der Zahlen } (1,0),\ (2,0) \text{ mit } (12,0) \\ \text{„ „ } (1,0),\ (2,0),\ (3,0) \text{ mit } (123,0) \\ \text{„ „ } (1,0),\ (2,0),\ (3,0),\ (4,0) \text{ mit } (1234,0) \end{array}\right\} \quad (2)$$

u. s. w.,

wobei natürlich alle Ziffern mit einander vertauscht werden dürfen. Beschränken wir uns auf den nächsten Fall, wo *vier* Zahlen gegeben sind, so entstehen auf diese Weise elf grösste gemeinsame Theiler, nämlich sechs von der Form (12,0), vier von der Form (123,0), und einer von der Form (1234,0). Dieser letzte ist offenbar zugleich der grösste gemeinsame Theiler von je zweien der Form (123,0), (124,0), und folglich kann man

$$\left.\begin{array}{l} (123,0) = (1234,0)\,(123,4) \\ (124,0) = (1234,0)\,(124,3) \\ (134,0) = (1234,0)\,(134,2) \\ (234,0) = (1234,0)\,(234,1) \end{array}\right\} \quad (3)$$

setzen, wo die vier ganzen Zahlen

$$(123,4),\ (124,3),\ (134,2),\ (234,1) \quad (4)$$

relative Primzahlen sind. Hieraus folgt z. B., dass das Product

$$(1234,0)\ (123,4)\ (124,3)$$

das kleinste gemeinsame Vielfache der beiden Zahlen (123,0), (124,0) ist; da andererseits diese letzteren Zahlen beide Theiler von (1,0) und (2,0), also auch Theiler von deren grösstem gemeinsamen Theiler (12,0) sind, so muss der letztere auch durch das vorstehende Product theilbar sein. Man erhält daher die Zerlegungen

$$\left.\begin{array}{l} (12,0) = (1234,0)\ (123,4)\ (124,3)\ (12,34) \\ (13,0) = (1234,0)\ (123,4)\ (134,2)\ (13,24) \\ (14,0) = (1234,0)\ (124,3)\ (134,2)\ (14,23) \\ (23,0) = (1234,0)\ (123,4)\ (234,1)\ (23,14) \\ (24,0) = (1234,0)\ (124,3)\ (234,1)\ (24,13) \\ (34,0) = (1234,0)\ (134,2)\ (234,1)\ (34,12) \end{array}\right\} \quad (5)$$

in welchen sechs neue ganze Zahlen

$$\left.\begin{array}{l} (12,34),\ (13,24),\ (14,23) \\ (34,12),\ (24,13),\ (23,14) \end{array}\right\} \quad 6)$$

auftreten. Setzt man nun

$$a = (12,0),\quad b = (13,0),\quad c = (14,0),$$

und wendet man auf diese drei Zahlen die Betrachtungen und Bezeichnungen des §. 1 an mit Rücksicht auf (2), (3), (5), so ergiebt sich

$$\begin{array}{l} a_1 = (134,0),\quad b_1 = (124,0),\quad c_1 = (123,0),\quad d = (1234,0), \\ a' = (134,2),\quad b' = (124,3),\quad c' = (123,4), \\ a'' = (12,34),\quad b'' = (13,24),\quad c'' = (14,23), \end{array}$$

also

$$m = (1234,0)\ (123,4)\ (124,3)\ (134,2)\ (12,34)\ (13,24)\ (14,23).$$

Da nun die Zahl (1,0) zufolge (2) durch jede der drei Zahlen a, b, c, also auch durch deren kleinstes gemeinsames Vielfaches m theilbar ist, so erhält man schliesslich die folgenden Zerlegungen

$$\left.\begin{array}{l} (1,0) = (1234,0)\ (123,4)\ (124,3)\ (134,2)\ (12,34)\ (13,24)\ (14,23)\ (1,234) \\ (2,0) = (1234,0)\ (123,4)\ (124,3)\ (234,1)\ (12,34)\ (23,14)\ (24,13)\ (2,134) \\ (3,0) = (1234,0)\ (123,4)\ (134,2)\ (234,1)\ (13,24)\ (23,14)\ (34,12)\ (3,124) \\ (4,0) = (1234,0)\ (124,3)\ (134,2)\ (234,1)\ (14,23)\ (24,13)\ (34,12)\ (4,123) \end{array}\right\} \quad (7)$$

in welchen abermals vier neue ganze Zahlen

$$(1,234),\ (2,134),\ (3,124),\ (4,123) \qquad (8)$$

auftreten. Aus (3), (5), (7) ergeben sich umgekehrt die Darstellungen der in (4), (6), (8) bezeichneten vierzehn Zahlen durch die fünfzehn in (1) und (2) definirten Zahlen; man erhält z. B.

$$(123,4) = \frac{(123,0)}{(1234,0)} \qquad (9)$$

$$(12,34) = \frac{(12,0)\ (1234,0)}{(123,0)\ (124,0)} \qquad (10)$$

$$(1,234) = \frac{(1,0)\ (123,0)\ (124,0)\ (134,0)}{(12,0)\ (13,0)\ (14,0)\ (1234,0)} \qquad (11)$$

Fügen wir zu diesen Gleichungen noch die selbstverständliche

$$(1234,0) = (1234,0) \qquad (12)$$

hinzu, und nennen wir (wie in §. 1) die fünfzehn Zahlen (4), (6), (8), (12) die *Kerne* des Systems (1) der vier gegebenen Zahlen, so erscheint jede der letzteren in (7) als Product von acht Kernen, und ebenso erscheinen in den Gleichungen (5), (3), (12) die aus den gegebenen Zahlen gebildeten grössten gemeinsamen Theiler (2) als Producte von Kernen, während umgekehrt die fünfzehn Kerne in den Gleichungen (9), (10), (11), (12) durch die fünfzehn Zahlen (1) und (2) ausgedrückt sind.

§. 3. Combinationen.

Um diese Betrachtungen auf ein beliebiges System von n gegebenen Zahlen

$$(1,0), (2,0) \ldots (n,0)$$

auszudehnen, und um ihnen zugleich eine viel allgemeinere Bedeutung unterzulegen, ist es nöthig, einige Bemerkungen über die *Combinationen* α, β, γ ... vorauszuschicken, welche sich aus dem System der n verschiedenen *Elemente*

$$1, 2 \ldots n$$

bilden lassen. Die letzteren, welche hier nicht als Zahlen, sondern nur als Unterscheidungszeichen aufzufassen sind und durch irgend welche andere Zeichen ersetzt werden dürften, bilden zugleich die Combinationen *ersten Grades*. Jedes System α von r verschiedenen solchen Elementen heisst bekanntlich eine Combination $r$ten Grades; hierbei kommt es auf die Reihenfolge, in welcher die Elemente des Systems α genannt oder geschrieben werden, gar nicht an, und man kann die Combination selbst (wie in §. 2) am einfachsten durch die natürliche Folge ihrer Elemente bezeichnen, so dass z. B. 235 die aus den drei Elementen 2, 3, 5 bestehende Combination bedeutet; wenn freilich $n > 9$ ist, so müssen die Elemente einer Combination deutlicher von einander getrennt werden. Eine Combination α ist also bestimmt, wenn über jedes der n Elemente $1, 2 \ldots n$ die Entscheidung getroffen ist, ob es in α aufgenommen wird oder nicht; lässt man daher — was bekanntlich sehr zweckmässig ist — auch die leere Combination 0ten Grades zu, welche gar kein Element enthält und im Folgenden immer mit 0 bezeichnet werden soll, so ist 2^n die Anzahl aller verschiedenen Combinationen. Wenn jedes Element von α auch Element der Combination β ist, so heisst α ein *Theil* von β, und wenn zugleich β auch ein Theil von α ist, so ist α identisch mit β, was immer durch $\alpha = \beta$ ausgedrückt wird. Die Combination 0 ist ein Theil von *jeder* Combination.

Unter der *Summe* $\alpha + \beta$ von zwei Combinationen α, β soll die Combination verstanden werden, welche aus allen in α oder in β (oder in beiden) enthaltenen Elementen *besteht*, während ihr *Durchschnitt* $\alpha - \beta$ aus denjenigen Elementen bestehen soll, welche beiden Combinationen α, β gemeinsam angehören; ist kein solches gemeinsames Element vorhanden, also $\alpha - \beta = 0$, so sollen α, β *fremde* Combinationen heissen. Die Combination 0 ist fremd zu *jeder* Combination.

Um diese einfachen Begriffe durch ein Beispiel zu erläutern, wähle ich die drei Combinationen

$$\alpha = 2347, \quad \beta = 1357, \quad \gamma = 1267;$$

dann wird

$$\begin{array}{lll} \beta + \gamma = 123567, & \gamma + \alpha = 123467, & \alpha + \beta = 123457, \\ \beta - \gamma = 17, & \gamma - \alpha = 27, & \alpha - \beta = 37. \end{array}$$

Man überzeugt sich nun ohne Weiteres, dass für diese beiden Operationen $\pm$ die folgenden sechs *Fundamentalgesetze* gelten, deren Inbegriff wir mit A bezeichnen wollen:

$$\begin{array}{rl} \alpha + \beta = \beta + \alpha & (1') \\ \alpha - \beta = \beta - \alpha & (1'') \\ (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) & (2') \\ (\alpha - \beta) - \gamma = \alpha - (\beta - \gamma) & (2'') \\ \alpha + (\alpha - \beta) = \alpha & (3') \\ \alpha - (\alpha + \beta) = \alpha & (3'') \end{array}$$

Die vier Doppelgesetze (1), (2) spricht man bekanntlich so aus, dass jede der beiden Operationen symmetrisch (commutativ) und associativ ist, und hieraus folgt (vergl. D., §. 2), dass die Bildung der Summe oder des Durchschnittes von drei oder mehr Combinationen von der Reihenfolge ganz unabhängig ist, nach welcher man immer ein Paar der vorhandenen Combinationen auswählt, um daraus die Summe oder den Durchschnitt zu bilden. Durch das letzte Doppelgesetz (3) treten aber die beiden Operationen in eine dualistische Verbindung, aus welcher zunächst

$$\begin{array}{rl} \alpha + \alpha = \alpha & (4') \\ \alpha - \alpha = \alpha & (4'') \end{array}$$

folgt; denn (4') geht unmittelbar aus (3') hervor, wenn man β durch $(\alpha + \beta)$ ersetzt und (3'') berücksichtigt, und in ähnlicher Weise folgt (4'') aus (3'').

Nun leuchtet freilich die Wahrheit dieses abgeleiteten Doppelgesetzes (4) auch unmittelbar aus dem Begriffe der Operationen $\pm$ ein, aber diese Ableitbarkeit ist doch an sich nicht ohne Bedeutung. Ganz anders verhält es sich nämlich mit dem folgenden Doppelgesetz

$$\begin{array}{rl} (\alpha - \beta) + (\alpha - \gamma) = \alpha - (\beta + \gamma) & (5') \\ (\alpha + \beta) - (\alpha + \gamma) = \alpha + (\beta - \gamma) & (5'') \end{array}$$

welches aus den obigen sechs Fundamentalgesetzen A schlechterdings *nicht* ableitbar ist, wie später (in §. 4) noch weiter besprochen werden soll; hier ist es vielmehr erforderlich, nochmals auf die Bedeutung der Symbole zurückzugehen. Bedeutet μ die linke, ν die rechte Seite der Gleichung (5′), so haben wir zu zeigen, dass jedes Element μ' von μ auch in ν, und ebenso, dass jedes Element ν' von ν auch in μ enthalten ist. Zufolge des Summenbegriffes ist μ' in $(\alpha - \beta)$ oder in $(\alpha - \gamma)$ enthalten, und da der Satz zufolge (1′) symmetrisch in Bezug auf β, γ ist, so dürfen wir das Erstere annehmen; dann ist μ' gemeinsames Element von α und β, und da jedes Element von β auch in $(\beta + \gamma)$ enthalten ist, so ist μ' auch in dem Durchschnitte ν der Combinationen α und $(\beta + \gamma)$ enthalten. Umgekehrt, jedes Element ν' dieses Durchschnittes ν ist gewiss in α und ausserdem in β oder γ, also in einem der beiden Durchschnitte $(\alpha - \beta)$, $(\alpha - \gamma)$, mithin auch in deren Summe μ enthalten, w. z. b. w.

Auf ganz ähnliche Weise liesse sich der Satz (5″) beweisen, was wir dem Leser überlassen; aber es ist bemerkenswerth, dass dieser Satz schon eine *nothwendige Folge* des Satzes (5′) und der Gesetze A ist. Ersetzt man nämlich α, β, γ in (5′) resp. durch $\alpha + \gamma$, α, β, so folgt

$$[(\alpha + \gamma) - \alpha] + [(\alpha + \gamma) - \beta] = (\alpha + \gamma) - (\alpha + \beta),$$

was zufolge A zunächst die Form

$$(\alpha + \beta) - (\alpha + \gamma) = \alpha + [\beta - (\alpha + \gamma)] \qquad (6'')$$

annimmt; da ferner aus (5′), wenn α mit β vertauscht wird, sich

$$\beta - (\alpha + \gamma) = (\alpha - \beta) + (\beta - \gamma)$$

ergiebt, so geht vermöge A die rechte Seite von (6″) in

$$\alpha + [(\alpha - \beta) + (\beta - \gamma)] = [\alpha + (\alpha - \beta)] + (\beta - \gamma) = \alpha + (\beta - \gamma)$$

über, womit der Satz (5″) bewiesen ist.

Da das System A in dem Sinne dualistisch ist, dass es sich durch die Vertauschung der beiden Operationen $\pm$ vollständig reproducirt, so ist offenbar der Satz (5′) umgekehrt eine nothwendige Folge von (5″) und A; wollte man dies, was aber nicht mehr nöthig ist, auf dieselbe Weise wie oben darthun, so würde der Weg über den Zwischensatz

$$(\alpha - \beta) + (\alpha - \gamma) = \alpha - [\beta + (\alpha - \gamma)] \qquad (6')$$

führen, welcher das Gegenstück zu dem Satze (6″) bildet.

Auf die allgemeinen Beziehungen zwischen den Gesetzen A und den vier Sätzen (5), (6) werde ich im folgenden §. 4 noch näher eingehen, obgleich diese Untersuchung für unseren eigentlichen Gegenstand nicht erforderlich ist. Dagegen werden wir später (in §§. 7, 8) Gebrauch zu machen haben von dem folgenden

Satz. Genügen die vier Combinationen α, β, γ, δ der Bedingung

$$\alpha + \beta = \gamma + \delta \qquad (7)$$

so giebt es immer drei Combinationen ϱ, σ, ω, *welche den Bedingungen*

$$\beta = \varrho + \omega, \quad \delta = \sigma + \omega \tag{8}$$

$$\alpha + \varrho = \gamma + \sigma = \alpha + \gamma \tag{9}$$

genügen.

Der *Beweis* ergiebt sich unmittelbar aus den obigen Sätzen, ohne dass es nöthig wäre, auf die Bedeutung unserer Zeichen zurückzukommen. Setzt man nämlich

$$\varrho = \beta - \gamma, \quad \sigma = \alpha - \delta, \quad \omega = \beta - \delta$$

und

$$\tau = \alpha - \gamma,$$

so fliessen aus dem Satze (5′) in Verbindung mit der Annahme (7) und mit dem Satze (3″) die Relationen

$$\begin{aligned}
\sigma + \tau &= \alpha - (\gamma + \delta) = \alpha - (\alpha + \beta) = \alpha, \\
\varrho + \omega &= \beta - (\gamma + \delta) = \beta - (\alpha + \beta) = \beta, \\
\varrho + \tau &= \gamma - (\alpha + \beta) = \gamma - (\gamma + \delta) = \gamma, \\
\sigma + \omega &= \delta - (\alpha + \beta) = \delta - (\gamma + \delta) = \delta,
\end{aligned}$$

deren zweite und vierte mit (8) übereinstimmen, während aus den beiden anderen folgt, dass jede der drei in (9) auftretenden Combinationen $= \varrho + \sigma + \tau$ ist, w. z. b. w.

Der Vollständigkeit wegen erwähnen wir ferner, dass offenbar immer

$$\alpha + 0 = \alpha, \quad \alpha - 0 = 0 \tag{10}$$

ist, und um die späteren Untersuchungen nicht zu unterbrechen, fügen wir noch folgende Bemerkungen hinzu. Nennt man eine Combination *paar* oder *unpaar*, je nachdem ihr *Grad* gerade oder ungerade ist, so besitzt jede Combination α, deren Grad $r > 0$ ist, offenbar ebenso viele paare wie unpaare *Theile*, nämlich 2^{r-1}; die ersteren, zu denen immer die Combination 0 gehört, sollen mit α'', die letzteren mit α' bezeichnet werden. Die Combination 0 dagegen besitzt nur einen einzigen, und zwar paaren Theil, nämlich 0 selbst. Sind nun α, β irgend zwei *fremde* Combinationen, ist also $\alpha - \beta = 0$, so leuchtet ein, dass die paaren Theile $(\alpha + \beta)''$ der Summe $(\alpha + \beta)$ mit allen Combinationen von der Form $\alpha'' + \beta''$ und von der Form $\alpha' + \beta'$, und dass die unpaaren Theile $(\alpha + \beta)'$ mit allen Combinationen von der Form $\alpha' + \beta''$ und von der Form $\alpha'' + \beta'$ übereinstimmen; auch ist jeder Theil von $\alpha + \beta$ nur in einer dieser vier Formen, und zwar nur auf eine einzige Weise darstellbar. Ist ferner $\beta = 0$, so fallen die Formen aus, in welchen β' auftritt.

§. 4. Bemerkungen über Dualgruppen.

Die im vorhergehenden §. 3 enthaltenen Betrachtungen sind ihrem grössten Theile nach keineswegs neu; da eine Combination nichts Anderes als ein System von Elementen ist, so gehören sie in die

allgemeine *Systemlehre*, welche wohl am vollständigsten in dem umfassenden und durch eine Fülle origineller Betrachtungen fesselnden Werke: *Die Algebra der Logik* von *E. Schröder*, behandelt ist. Zur Erleichterung der Vergleichung mache ich darauf aufmerksam, dass der Durchschnitt $\alpha - \beta$ der Systeme α, β in diesem Werke das *Product* von α, β genannt und demgemäss mit $\alpha\beta$ bezeichnet wird; diese Ausdrucks- und Bezeichnungsweise mag manche Vorzüge besitzen, doch schien mir die meinige für den gegenwärtigen Zweck hauptsächlich deshalb geeigneter, weil hier eine Uebereinstimmung mit der in der Modul- und Idealtheorie von mir eingeführten Bezeichnungsart wünschenswerth war. Hiernach entsprechen die in §. 3 mit (1), (2), (3), (4), (5) bezeichneten Doppelsätze resp. den Doppelsätzen (12), (13), (23), (14), (27) auf S. 254, 255, 276, 259, 282 im ersten Bande des genannten Werkes; im Folgenden wird meine Bezeichnung der Sätze beibehalten, und unter A ist immer das System der Doppelsätze (1), (2), (3) zu verstehen, deren nothwendige Folge der Doppelsatz (4) ist.

Auf S. 292 bis 293 zeigt Herr Schröder ebenfalls, aber auf etwas andere Weise, als es hier in §. 3 geschehen ist, dass jeder der beiden Sätze (5) auf den anderen vermöge des Systems A zurückführbar ist. Von besonderem Interesse ist aber die zuerst auf S. 286 ausgesprochene, später auf S. 643 und abermals auf S. 686 bewiesene Behauptung, *dass keiner der beiden Sätze (5) eine nothwendige Folge des Systems A ist.*

Seit vielen Jahren habe ich mich ebenfalls mit diesen Fragen beschäftigt; doch hat mich hierzu nicht das Studium der Logik, sondern die Theorie derjenigen Zahlensysteme veranlasst, welche ich *Moduln* nenne[1]). Bei dem Bestreben, diese Theorie auf die kleinste Anzahl von Grundgesetzen zurückzuführen, habe ich ebenfalls — nicht ohne grosse Anstrengung — die eben erwähnte Thatsache erkannt, und da der von mir eingeschlagene Weg vielleicht noch einiges Neue enthält, auch wohl etwas einfacher zu sein scheint, als die von Herrn Schröder gegebenen Beweise, die er selbst als nicht mühelose bezeichnet, so erlaube ich mir, aus einer grösseren, halb vollendeten Abhandlung einige Betrachtungen hier mitzutheilen, obgleich sie für den vorliegenden Aufsatz nicht erforderlich sind. Zuvor bemerke ich, dass selbstverständlich die Priorität für die Entdeckung der genannten Thatsache durchaus Herrn Schröder gebührt; auch muss ich gestehen, dass es mir noch nicht gelungen ist, die späteren Bände seines grossen Werkes vollständig durchzuarbeiten, und so muss ich um Nachsicht bitten, wenn manche der folgenden Betrachtungen, bei welchen ich die leicht zu findenden Beweise grösstentheils unterdrücke, schon bekannt sein sollten. Ich beginne mit der folgenden Erklärung.

[1]) Vergl. S. 442, 479, 493 der zweiten, dritten, vierten Auflage von Dirichlet's Vorlesungen über Zahlentheorie.

Ein System $\mathfrak{A}$ von irgend welchen Dingen α, β, γ ... soll eine *Dualgruppe* heissen, wenn es zwei Operationen $\pm$ giebt, welche aus je zwei Dingen α, β zwei ebenfalls in $\mathfrak{A}$ enthaltene Dinge $\alpha \pm \beta$ erzeugen und zugleich den Bedingungen A genügen.

Um zu zeigen, wie verschiedenartig die Gebiete sind, auf welche dieser Begriff angewendet werden kann, erwähne ich folgende Beispiele:

1. Das nächste und überall unentbehrliche Beispiel liefert die oben erwähnte Systemlehre der Logik; bedeuten die Dinge α, β, γ ... endliche oder unendliche Systeme (Combinationen) von Elementen, und bezeichnet man mit $\alpha + \beta$ die logische Summe, mit $\alpha - \beta$ den Durchschnitt (das logische Product $\alpha\beta$ nach Schröder) von α, β, so bildet der Inbegriff $\mathfrak{A}$ aller Systeme α, β, γ ... eine Dualgruppe.

2. Der Inbegriff $\mathfrak{A}$ aller Zahlensysteme α, β, γ ..., welche ich *Moduln* nenne, bildet eine Dualgruppe, wenn unter $\alpha + \beta$ der grösste gemeinsame Theiler, unter $\alpha - \beta$ das kleinste gemeinsame Vielfache der beiden Moduln α, β verstanden wird. Dies Beispiel ist keineswegs in dem vorigen enthalten; denn hier enthält der Modul $\alpha + \beta$ ausser den in α oder β enthaltenen Zahlen (im Allgemeinen) noch unendlich viele andere Zahlen (Elemente), während $\alpha - \beta$ auch hier der Durchschnitt der Systeme α, β, d. h. der Inbegriff aller den Moduln α, β gemeinsamen Zahlen ist.

3. Einen speciellen Fall der Moduln bilden die *Ideale*[1]) α, β, γ ... eines endlichen Körpers, und da die daraus erzeugten Ideale $\alpha \pm \beta$ demselben Körper angehören, so ist der Inbegriff $\mathfrak{A}$ aller dieser Ideale eine Dualgruppe.

4. Ist ω eine endliche oder unendliche[2]) *Abel'sche* oder auch *Galois'sche Gruppe*, so bildet der Inbegriff $\mathfrak{A}$ aller Gruppen α, β, γ ..., welche als Theiler in ω enthalten sind (und zu denen auch ω selbst gehört), eine Dualgruppe, wenn unter $\alpha + \beta$ das kleinste gemeinsame Vielfache, unter $\alpha - \beta$ der grösste gemeinsame Theiler der beiden Gruppen α, β verstanden wird.

5. Der Inbegriff $\mathfrak{A}$ aller Zahlensysteme α, β, γ ..., welche ich *Körper*[3]) nenne, bildet eine Dualgruppe, wenn unter $\alpha + \beta$ das kleinste gemeinsame Multiplum, unter $\alpha - \beta$ der grösste gemeinsame Divisor der beiden Körper α, β verstanden wird.

6. Als letztes Beispiel mag das folgende dienen. Unter einem *Punkte* α des reellen Zahlenraumes von n Dimensionen sei jede Folge von n reellen Zahlen α_1, α_2 ... α_n verstanden, welche umgekehrt die erste, zweite ... $n$te Coordinate des Punktes α heissen mögen; definirt

[1]) Vergl. S. 452, 508, 551 der zweiten, dritten, vierten Auflage von Dirichlet's Zahlentheorie.

[2]) Vergl. §. 5 dieses Aufsatzes.

[3]) Vergl. S. 424, 435, 452 der zweiten, dritten, vierten Auflage von Dirichlet's Zahlentheorie.

man nun für je zwei Punkte α, β die Punkte $\alpha \pm \beta$ dadurch, dass die Coordinate $(\alpha + \beta)_r$ die algebraisch grösste, die Coordinate $(\alpha - \beta)_r$ die algebraisch kleinste der beiden Coordinaten α_r, β_r sein soll, so bildet der *Raum* $\mathfrak{A}$ als Inbegriff aller Punkte α, β, $\gamma \ldots$ eine Dualgruppe.

Wir wenden uns nun zur Untersuchung über die Gültigkeit der in §. 3 mit (5) und (6) bezeichneten Doppelsätze innerhalb der allgemeinen Theorie der Dualgruppen. Es ist dort schon gezeigt, dass die beiden Sätze (5′) und (5″) vermöge der Grundgesetze A wechselseitig aus einander folgen; dieses Doppelgesetz (5) gilt zufolge §. 3 wirklich in dem ersten der eben aufgeführten Beispiele, in der Systemlehre der Logik; es gilt [1]) aber auch in dem dritten Beispiele, in der aus allen Idealen eines endlichen Körpers bestehenden Dualgruppe; aus diesem Grunde will ich diesen Doppelsatz (5) hier das *Idealgesetz* nennen, und jede Dualgruppe, in welcher dies Gesetz gilt, mag eine Dualgruppe vom *Idealtypus* heissen.

Von ebenso grosser Wichtigkeit sind aber auch die in §. 3 mit (6′) und (6″) bezeichneten Sätze, sowie der folgende, bisher noch nicht erwähnte Satz

$$[\alpha + (\beta - \gamma)] - (\beta + \gamma) = [\alpha - (\beta + \gamma)] + (\beta - \gamma) \quad (M)$$

welcher symmetrisch in Bezug auf β, γ und zugleich sein eigenes dualistisches Gegenstück ist. Ich bemerke zunächst, dass je zwei dieser drei Sätze (6′), (6″), (M) äquivalent sind, d. h. wechselseitig vermöge der Grundgesetze A aus einander folgen. Bezeichnet man nämlich kurz mit (λ, μ, ν) eine Substitution, welche darin besteht, dass die drei Dinge α, β, γ resp. durch die drei Dinge λ, μ, ν ersetzt werden so überzeugt man sich leicht, dass

(6′)	durch	$(\alpha + \gamma,\ \beta,\ \alpha)$	in	(6″)
(6″)	„	$(\alpha - \gamma,\ \beta,\ \alpha)$	„	(6′)
(6′)	„	$(\beta + \gamma,\ \alpha,\ \beta - \gamma)$	„	(M)
(M)	„	$(\beta,\ \alpha,\ \alpha - \gamma)$	„	(6′)
(6″)	„	$(\beta - \gamma,\ \alpha,\ \beta + \gamma)$	„	(M)
(M)	„	$(\beta,\ \alpha,\ \alpha + \gamma)$	„	(6″)

übergeht. Dieses dreiförmige Gesetz gilt [2]) nun wirklich in dem zweiten der obigen Beispiele, in der aus allen Moduln bestehenden Dualgruppe; ich will es daher das *Modulgesetz* nennen, und jede Dualgruppe, in welcher es herrscht, mag eine Dualgruppe vom *Modultypus* heissen.

[1]) Dies folgt leicht aus D., §. 178.

[2]) Vergl. D., §. 169; die dortigen Sätze (7), (8), (8′) stimmen resp. überein mit den obigen (M), (6″), (6′); zuerst erwähnt sind sie auf S. 17 meiner Schrift: Ueber die Anzahl der Idealclassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig 1877).

Da ferner in §. 3 die Sätze (6′), (6″) lediglich vermöge der Grundgesetze A aus den Sätzen (5″), (5′) abgeleitet sind, so leuchtet die Wahrheit der folgenden Behauptung ein:

Jede Dualgruppe vom Idealtypus besitzt auch den Modultypus.

Hiernach entspringen naturgemäss die beiden Fragen:

Giebt es Dualgruppen, welche den Modultypus nicht besitzen?

Giebt es Dualgruppen vom Modultypus, welche den Idealtypus nicht besitzen?

Dass diese Fragen beide zu *bejahen* sind, habe ich — nicht ohne Mühe — dadurch entschieden, dass ich mir die bestimmte Aufgabe stellte, jedesmal die *kleinste* Dualgruppe aufzusuchen, welche die fragliche Eigenschaft hat. Die auf diese Weise gefundenen Gruppen bestehen aus je *fünf verschiedenen* Dingen, α, β, γ, δ, ε, und sind in den beiden folgenden Tabellen dargestellt:

	α	β	γ	δ	ε
α		δ	γ	δ	α
β	ε		δ	δ	β
γ	α	ε		δ	γ
δ	α	β	γ		δ
ε	ε	ε	ε	ε	

	α	β	γ	δ	ε
α		δ	δ	δ	α
β	ε		δ	δ	β
γ	ε	ε		δ	γ
δ	α	β	γ		δ
ε	ε	ε	ε	ε	

Zur Erläuterung dienen folgende Bemerkungen. Bedeutet (μ, ν) den Buchstaben, welcher sich im Durchschnittsfelde der Zeile μ und der Spalte ν findet, so hätten die Felder der Diagonale eigentlich mit den Buchstaben $(\mu, \mu) = \mu$ besetzt werden sollen; des deutlicheren Ueberblickes wegen sind sie aber leer gelassen, um die oberhalb und unterhalb der Diagonale gelegenen Hälften der Tabellen für das Auge leichter zu trennen; in der oberen Hälfte finden sich die Buchstaben $(\mu, \nu) = \mu + \nu = \nu + \mu$, in der unteren die Buchstaben $(\mu, \nu) = \mu - \nu = \nu - \mu$. Die durch die richtigen Buchstaben $(\mu, \mu) = \mu = \mu + \mu = \mu - \mu$ besetzt zu denkenden Diagonalfelder gehören sowohl zu der oberen wie zu der unteren Hälfte. Die Tabellen enthalten daher für beide Operationen $\pm$ die vollständige Anweisung zu ihrer Ausführung.

Die genaue Prüfung ergiebt, dass in beiden Tabellen die Grundgesetze A, in der zweiten auch die Gesetze (6′), (6″) erfüllt sind; das System $\mathfrak{A}$ der fünf Dinge α, β, γ, δ, ε bildet daher in beiden Beispielen

eine Dualgruppe, und die zweite dieser beiden Dualgruppen besitzt den Modultypus. Aus der ersten Tabelle folgt nun

$$(\alpha + \beta) - (\alpha + \gamma) = \delta - \gamma = \gamma,$$
$$\alpha + [\beta - (\alpha + \gamma)] = \alpha + (\beta - \gamma) = \alpha + \varepsilon = \alpha,$$

mithin gilt in der ersten Dualgruppe das Modulgesetz (6″) *nicht*. Aus der zweiten Tabelle folgt

$$(\alpha + \beta) - (\alpha + \gamma) = \delta - \delta = \delta,$$
$$\alpha + (\beta - \gamma) = \alpha + \varepsilon = \alpha,$$

mithin gilt in der zweiten Dualgruppe das Idealgesetz (5″) *nicht*. Hiermit sind die obigen Behauptungen gerechtfertigt.

Die eben dem Leser überlassene Prüfung, ob die durch die Tabellen definirten Operationen $\pm$ innerhalb eines Systems $\mathfrak{A}$ den Grundgesetzen A, eventuell auch dem Modulgesetz genügen, erweist sich bei der wirklichen Ausführung schon bei diesen einfachen Beispielen, wo das System $\mathfrak{A}$ endlich ist und nur aus fünf verschiedenen Dingen besteht, als ziemlich mühsam. Dies veranlasst mich, hier noch eine *Transformation der Grundgesetze A* zu besprechen, durch welche deren Prüfung im Allgemeinen wohl etwas erleichtert wird, und die zugleich ein neues Licht auf das Wesen der Dualgruppen wirft.

Ist α ein bestimmtes Ding in einer Dualgruppe $\mathfrak{A}$, so will ich mit α' das *System* aller in der Form $\alpha + \omega$ darstellbaren Dinge α_1 bezeichnen [1]), wo ω jedes Ding in $\mathfrak{A}$ bedeuten kann. Diese Systeme von der Form α' besitzen die folgenden sechs charakteristischen Eigenschaften, in welchen die beiden Operationen $\pm$ gar nicht mehr auftreten:

I. Jedem Dinge α in $\mathfrak{A}$ entspricht ein vollständig bestimmter Theil α' von $\mathfrak{A}$.

II. Das Ding α ist in α' enthalten.

III. Aus $\alpha' = \beta'$ folgt $\alpha = \beta$.

IV. Ist das Ding α_1 in α' enthalten, so ist das System α_1' ein Theil von α'.

V. Der Durchschnitt von je zwei Systemen α', β' (d. h. der Inbegriff aller ihnen gemeinsamen Dinge) ist selbst wieder ein System ν'.

VI. Für je zwei Dinge α, β in $\mathfrak{A}$ giebt es ein Ding μ in $\mathfrak{A}$, welches den beiden folgenden Bedingungen genügt: α' und β' sind Theile von μ', und wenn α', β' Theile von einem System μ_2' sind, so ist auch μ' ein Theil von μ_2'.

---

[1]) Diese Systeme α' und die später folgenden Systeme α'' dürfen nicht mit den in §. 3 erklärten unpaaren und paaren Theilen einer Combination α verwechselt werden.

Dass wirklich diese Eigenschaften eine unmittelbare Folge der Grundgesetze A und der obigen Definition der Systeme α' sind, wird der Leser ohne jede Mühe finden, und zwar wird V. durch $\nu = \alpha + \beta$, und VI. durch $\mu = \alpha - \beta$ erfüllt.

Lässt man nun die Erinnerung an die Operationen $\pm$ gänzlich fallen, und nimmt man lediglich an, es gelten in einem Systeme $\mathfrak{A}$ die vorstehenden sechs Eigenschaften, so kann man den Systemen α' eine zweite Classe von Systemen α'' innerhalb $\mathfrak{A}$ gegenüberstellen, deren Erklärung die folgende ist. Bedeutet α irgend ein Ding in $\mathfrak{A}$, so giebt es zufolge II. mindestens ein Ding α_2 von der Art, dass α in α_2' enthalten ist, und mit α'' soll der Inbegriff aller dieser Dinge α_2 bezeichnet werden. Man wird sich leicht überzeugen, dass diese Systeme α'' (wenn man zugleich α_1, ν, μ, μ_2 resp. durch α_2, μ, ν, ν_1 ersetzt) genau *dieselben* sechs Eigenschaften besitzen, wie die Systeme α', und rückwärts ergiebt sich aus den Systemen α'', falls diese gegeben sind, auf dieselbe Weise wieder die Construction der Systeme α'.

Wenn nun in $\mathfrak{A}$ eine der beiden Classen von Systemen α', α'' und folglich auch die andere gegeben ist, so kann man in $\mathfrak{A}$ zwei Operationen $\pm$ eindeutig dadurch definiren, dass $\alpha + \beta = \nu$, $\alpha - \beta = \mu$ gesetzt wird, wo ν, μ die in V., VI. angegebene Bedeutung haben, und man zeigt leicht, dass diese Operationen die Grundgesetze A einer *Dualgruppe* $\mathfrak{A}$ erfüllen, und dass die Systeme α', α'' resp. die Inbegriffe aller in den Formen $\alpha + \omega$, $\alpha - \omega$ darstellbaren Dinge α_1, α_2 sind.

Aus diesem Kreislauf von den Operationen $\pm$ zu den Systemen α', α'', und zurück von diesen zu jenen ergiebt sich einerseits, dass in einer Dualgruppe $\mathfrak{A}$ nur die *eine* der beiden Operationen $\pm$ durch eine (endliche oder unendliche) Tabelle gegeben zu sein braucht, dass die *andere* hierdurch zugleich vollständig bestimmt ist. Dasselbe ergiebt sich übrigens auch ohne die Einführung der Systeme α', α'' leicht aus den Grundgesetzen A; nimmt man nämlich an, eine dritte Operation $|$ erfülle für sich allein und in Verbindung mit der Operation $+$ dieselben Gesetze A, wie die Operation $-$, so ergiebt sich, wie der Leser sogleich finden wird, dass immer $\alpha \mid \beta = \alpha - \beta$, also die Operation $|$ identisch mit $-$ sein muss.

Andererseits lehrt dieser Kreislauf, dass eine Dualgruppe $\mathfrak{A}$ statt durch eine Tabelle, in welcher die Resultate der Operationen $\pm$ oder vielmehr nur einer dieser Operationen dargestellt sind, auch auf ganz andere Art, nämlich durch Angabe aller Systeme α', oder aller Systeme α'' vollständig definirt werden kann.

So z. B. tritt an die Stelle der beiden obigen Tabellen (oder deren Hälften) je eine Hälfte der beiden folgenden Tabellen:

ω	ω'	ω''
α	α, γ, δ	α, ε
β	β, δ	β, ε
γ	γ, δ	$\alpha, \gamma, \varepsilon$
δ	δ	$\alpha, \beta, \gamma, \delta, \varepsilon$
ε	$\alpha, \beta, \gamma, \delta, \varepsilon$	ε

ω	ω'	ω''
α	α, δ	α, ε
β	β, δ	β, ε
γ	γ, δ	γ, ε
δ	δ	$\alpha, \beta, \gamma, \delta, \varepsilon$
ε	$\alpha, \beta, \gamma, \delta, \varepsilon$	ε

Diese Tabellen ergeben nun, ohne die Feder zu gebrauchen, durch den blossen Anblick der Zeilen die Bestätigung der obigen sechs Eigenschaften, also den Beweis, dass die beiden Systeme $\mathfrak{A}$ wirklich Dualgruppen sind, und es ist wohl anzunehmen, dass auch bei complicirteren Beispielen unsere zweite Art der Darstellung von Dualgruppen Vorzüge vor der früheren Art besitzen wird. Auch die Prüfung, ob eine Dualgruppe den Modultypus oder gar den Idealtypus besitzt, lässt sich wohl erleichtern, doch kann ich hierauf nicht mehr eingehen [1]).

Zum Schluss erwähne ich noch Folgendes. Ist α_1 in der Form $\alpha + \omega$ darstellbar, also in dem System α' enthalten, so folgt $\alpha + \alpha_1 = \alpha_1$ und hieraus $\alpha - \alpha_1 = \alpha - (\alpha + \alpha_1) = \alpha$; umgekehrt folgt auch $\alpha + \alpha_1 = \alpha_1$ aus $\alpha - \alpha_1 = \alpha$, und α ist in dem System α_1'' enthalten. Diese Beziehung zwischen zwei Dingen α, α_1 einer Dualgruppe $\mathfrak{A}$ tritt so häufig auf, dass eine noch kürzere Bezeichnung derselben wünschenswerth ist. In der aus allen *Moduln* bestehenden Dualgruppe $\mathfrak{A}$ habe ich hierfür die doppelte Bezeichnung [2])

$$\alpha > \alpha_1, \quad \alpha_1 < \alpha$$

eingeführt, die freilich bei der Uebertragung auf andere Beispiele von Dualgruppen dem Sinne, welcher sonst den Zeichen $>$, $<$ beigelegt wird, oft widersprechen mag, aber für die *allgemeine* Theorie doch ganz unbedenklich ist. Aus der grossen Anzahl von Sätzen über den Gebrauch dieser Zeichen erwähne ich erstens, dass aus $\alpha_1 < \alpha$ und $\alpha < \alpha_2$, was bequem in $\alpha_1 < \alpha < \alpha_2$ zusammengezogen werden kann, stets $\alpha_1 < \alpha_2$ folgt, und zweitens, dass aus $\alpha_1 < \alpha$ und $\alpha_1 > \alpha$ immer $\alpha_1 = \alpha$ folgt. Nun ist oben gezeigt, dass es Dualgruppen giebt, in welchen weder das Idealgesetz (5), noch das Modulgesetz (6) herrscht; dagegen gelten in *jeder* Dualgruppe die folgenden Gesetze

[1]) Vergl. D., §. 169, S. 499, Anmerkung.

[2]) D., §. 169, S. 495. Vergl. auch das oben citirte Werk von Schröder, S. 270, Satz (20).

$$(\alpha - \beta) + (\alpha - \gamma) > \alpha - [\beta + (\alpha - \gamma)]$$
$$(\alpha + \beta) - (\alpha + \gamma) < \alpha + [\beta - (\alpha + \gamma)]$$

und

$$\alpha - [\beta + (\alpha - \gamma)] > \alpha - (\beta + \gamma)$$
$$\alpha + [\beta - (\alpha + \gamma)] < \alpha + (\beta - \gamma),$$

also auch die beiden folgenden [1])

$$(\alpha - \beta) + (\alpha - \gamma) > \alpha - (\beta + \gamma)$$
$$(\alpha + \beta) - (\alpha + \gamma) < \alpha + (\beta - \gamma).$$

Die Herstellung der leicht zu findenden Beweise muss ich aber dem Leser überlassen.

§. 5. Abel'sche Gruppe $\mathfrak{G}$.

Nach dieser Abschweifung kehren wir zu der Aufgabe zurück, die wir in den §§. 1 und 2 für natürliche oder allgemeiner für (positive) rationale Zahlen behandelt haben. Diese Aufgabe soll aber jetzt in doppelter Weise verallgemeinert werden, zunächst dadurch, dass statt drei oder vier Zahlen beliebig viele in endlicher Anzahl n gegeben sein sollen, wobei uns die in §. 3 enthaltenen Betrachtungen über Combinationen nützliche Dienste leisten werden. Die zweite Art der Verallgemeinerung besteht darin, dass wir an Stelle der rationalen Zahlen die Elemente $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ... einer endlichen oder unendlichen *Abel'schen Gruppe* $\mathfrak{G}$ treten lassen. Wir setzen also voraus, es gebe eine, der Multiplication der Zahlen ähnliche Operation, welche aus je zwei Elementen $\mathfrak{a}$, $\mathfrak{b}$ der Gruppe $\mathfrak{G}$ ein in derselben enthaltenes Element $\mathfrak{a}\mathfrak{b}$ erzeugt; wir nennen diese Gruppenoperation unbedenklich eine *Multiplication* und das erzeugte Element $\mathfrak{a}\mathfrak{b}$ das *Product* aus den *Factoren* $\mathfrak{a}$, $\mathfrak{b}$. Ueber diese Operation machen wir drei Annahmen, deren *erste* darin besteht, dass das Commutations- und Associationsgesetz

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}, \quad (\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}) \tag{1}$$

erfüllt ist. Wir setzen *zweitens* voraus, es gebe in $\mathfrak{G}$ ein Element $\mathfrak{o}$, welches der Zahl 1 bei der Multiplication der Zahlen insofern entspricht, dass die Gleichung

$$\mathfrak{a}\mathfrak{o} = \mathfrak{a} \tag{2}$$

für jedes Element $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ gilt; es kann nur ein einziges solches Element $\mathfrak{o}$ geben, weil, wenn $\mathfrak{p}$ dieselbe Eigenschaft besitzt, $\mathfrak{o}\mathfrak{p}$ sowohl $= \mathfrak{p}$, wie $= \mathfrak{o}$ sein muss; dieses Element $\mathfrak{o}$ heisst das *Hauptelement* der Gruppe $\mathfrak{G}$. Unsere *dritte* und letzte Annahme besteht darin, dass zu jedem Elemente $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ ein *reciprokes*, mit $\mathfrak{a}^{-1}$ zu bezeichnendes Element von $\mathfrak{G}$ gehört, welches der Bedingung

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o} \tag{3}$$

[1]) Vergl. Satz (25) auf S. 280 des Werkes von Schröder.

genügt; es kann nur ein einziges solches Element geben, weil, falls $\mathfrak{a}\,\mathfrak{q} = \mathfrak{o}$ angenommen wird, das Product $\mathfrak{q}\,\mathfrak{a}\,\mathfrak{a}^{-1}$ sowohl $= (\mathfrak{q}\,\mathfrak{a})\,\mathfrak{a}^{-1} = \mathfrak{a}^{-1}$ wie $= \mathfrak{q}\,(\mathfrak{a}\,\mathfrak{a}^{-1}) = \mathfrak{q}$ ist. Offenbar ist $\mathfrak{a}$ das reciproke Element von $\mathfrak{a}^{-1}$, ferner $\mathfrak{o}^{-1} = \mathfrak{o}$.

Wir können nun auch eine der Gruppenoperation entgegengesetzte *Division* einführen; dies ist zwar für unseren Zweck nicht durchaus erforderlich, aber die Schreibweise mancher Formeln wird dadurch für das Auge übersichtlicher. Wir definiren daher den aus dem *Zähler* $\mathfrak{a}$ und dem *Nenner* $\mathfrak{b}$ gebildeten *Bruch* oder *Quotienten* durch

$$\mathfrak{a} : \mathfrak{b} = \frac{\mathfrak{a}}{\mathfrak{b}} = \mathfrak{a}\,\mathfrak{b}^{-1} \tag{4}$$

woraus

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)\mathfrak{b} = \mathfrak{a} \tag{5}$$

folgt. Zugleich leuchtet ein, dass alle Regeln der Multiplication, Division, Erweiterung und Hebung von Zahlbrüchen sich auf diese neuen Brüche übertragen, und dass jedes Element $\mathfrak{a}$ der Gruppe auch als Bruch $(\mathfrak{a} : \mathfrak{o})$ angesehen werden kann.

Es wird im Folgenden oft von Producten $\Pi\mathfrak{a}$ die Rede sein, wo das Productzeichen Π sich auf alle m Elemente $\mathfrak{a} = \mathfrak{a}_1, \mathfrak{a}_2 \ldots \mathfrak{a}_m$ bezieht, welche unter einer gemeinsamen Form enthalten sind oder gewissen Bedingungen genügen; ein solches Product ist also erklärt durch

$$\Pi\mathfrak{a} = \mathfrak{a}_1\,\mathfrak{a}_2 \ldots \mathfrak{a}_m \tag{6}$$

Es kommt aber auch vor, dass die Anzahl m der fraglichen Elemente $\mathfrak{a}$ auf 1 oder 0 herabsinkt, und wir wollen festsetzen, dass unter $\Pi\mathfrak{a}$ im ersten Falle immer das einzige Element $\mathfrak{a}_1$ selbst, im letzteren Falle immer das Hauptelement $\mathfrak{o}$ der Gruppe zu verstehen ist.

Dieselbe Regel soll auch für die *Potenz* $\mathfrak{a}^m$ gelten, d. h. für ein Product aus lauter *gleichen* Factoren $\mathfrak{a}$, deren Anzahl der *Exponent* m ist; es wird daher $\mathfrak{a}^1 = \mathfrak{a}$, und $\mathfrak{a}^0 = \mathfrak{o}$ zu setzen sein. Versteht man ferner unter einer Potenz $\mathfrak{a}^{-m}$ mit *negativem* Exponenten $(-m)$ die $m$te Potenz von $\mathfrak{a}^{-1}$, so gelten für Producte und Quotienten von Potenzen dieselben Regeln, wie in der Arithmetik. —

Nach diesen Vorbereitungen wenden wir uns zu unserem eigentlichen Gegenstande. Wir bezeichnen, wie in §. 3, mit $\alpha, \beta, \gamma \ldots$ alle Combinationen, welche sich aus den n Unterscheidungszeichen

$$1, 2 \ldots n \tag{7}$$

bilden lassen, und deren Anzahl $= 2^n$ ist. Für jede solche Combination α wählen wir *willkürlich* aus unserer Abel'schen Gruppe $\mathfrak{G}$ ein Element, welches wir durch

$$(\alpha, 0) \tag{8}$$

bezeichnen wollen[1]). Nachdem dies geschehen ist, definiren wir für jedes Paar von Combinationen α, β ein zugehöriges Element (α, β) der Gruppe $\mathfrak{G}$ durch

$$(\alpha, \beta) = \frac{\Pi(\alpha + \beta'', 0)}{\Pi(\alpha + \beta', 0)} \tag{9}$$

wo das Productzeichen Π sich im Zähler auf alle (in §. 3 definirten) *paaren* Theile β'', im Nenner auf alle *unpaaren* Theile β' der Combination β bezieht[2]).

Wir bemerken zunächst, dass nach den obigen Festsetzungen über den Gebrauch des Zeichens Π das in (9) definirte Element (α, β), falls $\beta = 0$ sein sollte, von selbst mit dem in (8) gewählten oder gegebenen Element $(\alpha, 0)$ identisch wird, weil es in diesem Falle gar kein unpaares β' und nur ein einziges paares $\beta'' = 0$ giebt. Ist ferner ε ein *Combinationselement*, d. h. eine der n Combinationen *ersten* Grades (7), so giebt es ein einziges unpaares $\varepsilon' = \varepsilon$ und ein einziges paares $\varepsilon'' = 0$, und aus der Definition (9) fliesst der Satz

$$(\alpha, 0) = (\alpha + \varepsilon, 0)\,(\alpha, \varepsilon) \tag{10}$$

welcher nur ein specieller Fall der späteren Sätze (12) und (13) ist. Wir stellen nun einige auf die Quotienten (9) bezügliche Sätze auf.

Satz I. Ist $\alpha - \beta$ von 0 verschieden, haben also α und β mindestens ein Element ε gemeinsam, so ist

$$(\alpha, \beta) = 0 \tag{11}$$

Beweis. Denn wenn man $\beta = \varepsilon + \omega$ setzt, wo ω das Element ε nicht enthält, so bestehen die paaren Theile β'' der Combination β theils aus allen paaren Theilen ω'' der Combination ω, theils aus allen Combinationen von der Form $\varepsilon + \omega'$, wo ω' jeden unpaaren Theil von ω bedeutet; ebenso bestehen die unpaaren Theile β' von β theils aus diesen Combinationen ω', theils aus allen Combinationen $\varepsilon + \omega''$. Bedenkt man nun, dass ε auch in α enthalten, also $\alpha + \varepsilon = \alpha$ ist, so bestehen die Combinationen $\alpha + \beta''$ aus allen $\alpha + \omega''$ und allen $\alpha + \omega'$, und ebenso bestehen die Combinationen $\alpha + \beta'$ aus allen $\alpha + \omega'$ und allen $\alpha + \omega''$; mithin ist das System der Combinationen $\alpha + \beta''$ identisch mit dem der Combinationen $\alpha + \beta'$, und zufolge der Definition (9) wird $(\alpha, \beta) = 0$, w. z. b. w.

Satz II. Ist ε eine Combination ersten Grades, so ist

$$(\alpha, \beta) = (\alpha + \varepsilon, \beta)\,(\alpha, \beta + \varepsilon) \tag{12}$$

Beweis. Falls ε in β enthalten, also $\beta + \varepsilon = \beta$ ist, leuchtet der Satz unmittelbar ein, weil nach dem vorhergehenden Satze $(\alpha + \varepsilon, \beta) = 0$ ist. Im entgegengesetzten Falle sind die paaren

---

[1]) Eine Beschränkung in der Freiheit dieser Wahl wird erst später in §. 7 eintreten.

[2]) Beispiele solcher Quotienten finden sich am Schlusse von §. 2.

Theile $(\beta + \varepsilon)''$ theils $= \beta''$, theils $= \varepsilon + \beta'$, und die unpaaren Theile $(\beta + \varepsilon)'$ theils $= \beta'$, theils $= \varepsilon + \beta''$; die Definition (9) giebt daher

$$(\alpha, \beta + \varepsilon) = \frac{\Pi(\alpha + \beta'', 0)\,\Pi(\alpha + \varepsilon + \beta', 0)}{\Pi(\alpha + \beta', 0)\,\Pi(\alpha + \varepsilon + \beta'', 0)},$$

woraus durch Vergleichung mit (9) und mit

$$(\alpha + \varepsilon, \beta) = \frac{\Pi(\alpha + \varepsilon + \beta'', 0)}{\Pi(\alpha + \varepsilon + \beta', 0)}$$

die Gleichung (12) folgt, w. z. b. w.

Satz III. Sind α, β, γ beliebige Combinationen, so ist

$$(\alpha, \beta) = \Pi(\alpha + \gamma_1, \beta + \gamma_2) \tag{13}$$

wo das Productzeichen Π sich auf alle verschiedenen Paare von Combinationen γ_1, γ_2 bezieht, die den Bedingungen

$$\gamma_1 + \gamma_2 = \gamma, \quad \gamma_1 - \gamma_2 = 0 \tag{14}$$

genügen.

Beweis. Der Satz gilt für $\gamma = 0$, weil in diesem Falle γ nur eine einzige Zerlegung $\gamma_1 = 0$, $\gamma_2 = 0$ besitzt; er gilt nach dem vorhergehenden Satze auch, wenn γ ein Combinationselement ist, weil dann γ nur die beiden Zerlegungen $\gamma_1 = \gamma$, $\gamma_2 = 0$ und $\gamma_1 = 0$, $\gamma_2 = \gamma$ besitzt. Der Inductionsbeweis wird daher vollendet sein, wenn wir annehmen, der Satz gelte für jede Combination γ vom Grade r, und hieraus seine Gültigkeit für jede Combination δ vom Grade $r + 1$ ableiten. Offenbar kann man $\delta = \gamma + \varepsilon$ setzen, wo ε ein beliebig gewähltes Element von δ bedeutet, während γ die aus den übrigen r Elementen von δ bestehende Combination ist. Behalten nun γ_1, γ_2 ihre obige Bedeutung, so zerfallen alle Paare δ_1, δ_2, welche den Bedingungen $\delta_1 + \delta_2 = \delta$, $\delta_1 - \delta_2 = 0$ genügen, in zwei verschiedene Arten, je nachdem das Element ε in δ_1 oder δ_2 aufgenommen wird; im ersten Falle ist $\delta_1 = \varepsilon + \gamma_1$, $\delta_2 = \gamma_2$, im zweiten $\delta_1 = \gamma_1$, $\delta_2 = \varepsilon + \gamma_2$, und folglich wird das auf alle Paare δ_1, δ_2 ausgedehnte Product

$$\Pi(\alpha + \delta_1, \beta + \delta_2) = \Pi(\alpha + \varepsilon + \gamma_1, \beta + \gamma_2)\,\Pi(\alpha + \gamma_1, \beta + \varepsilon + \gamma_2).$$

Da nach unserer Annahme der Satz (13) für jede Combination γ vom Grade r gilt, so ist auch

$$(\alpha + \varepsilon, \beta) = \Pi(\alpha + \varepsilon + \gamma_1, \beta + \gamma_2)$$
$$(\alpha, \beta + \varepsilon) = \Pi(\alpha + \gamma_1, \beta + \varepsilon + \gamma_2),$$

woraus mit Rücksicht auf den vorhergehenden Satz (12) sich

$$\Pi(\alpha + \delta_1, \beta + \delta_2) = (\alpha, \beta)$$

ergiebt, w. z. b. w.

Beispiele zu diesem, im Folgenden sehr häufig anzuwendenden Satze, den wir kurz den *Productsatz* nennen wollen, findet man in den Gleichungen (3), (5), (7) des §. 2. Wir wollen noch bemerken,

dass der Satz zufolge I auch dann gilt, wenn man die zweite der Bedingungen (14) fallen lässt; doch würde diese Verallgemeinerung nur eine scheinbare und kaum von Nutzen sein.

Satz IV. Sind α, β, γ beliebige Combinationen, so ist

$$(\alpha, \beta + \gamma) = \frac{\Pi(\alpha + \gamma'', \beta)}{\Pi(\alpha + \gamma', \beta)} \tag{15}$$

wo γ'' alle paaren, γ' alle unpaaren Theile von γ durchläuft.

Beweis. Der Satz gilt offenbar für $\gamma = 0$, weil es dann nur ein einziges $\gamma'' = 0$ und gar kein γ' giebt, also der Nenner $= 0$ wird. Gilt der Satz für jede Combination γ vom Grade r, und setzt man irgend eine Combination δ vom Grade $r + 1$ wieder in die Form $\gamma + \varepsilon$, wo ε ein Element von δ bedeutet, so bestehen die paaren Theile δ'' theils aus den Combinationen γ'', theils aus den Combinationen $\varepsilon + \gamma'$ und die unpaaren Theile δ' bestehen aus den Combinationen γ' und $\varepsilon + \gamma''$; mithin wird

$$\Pi(\alpha + \delta'', \beta) = \Pi(\alpha + \gamma'', \beta)\, \Pi(\alpha + \varepsilon + \gamma', \beta)$$
$$\Pi(\alpha + \delta', \beta) = \Pi(\alpha + \gamma', \beta)\, \Pi(\alpha + \varepsilon + \gamma'', \beta)$$

also nach unserer Inductionsannahme

$$\frac{\Pi(\alpha + \delta'', \beta)}{\Pi(\alpha + \delta', \beta)} = \frac{(\alpha, \beta + \gamma)}{(\alpha + \varepsilon, \beta + \gamma)},$$

und da die rechte Seite zufolge (12), wenn dort β durch $\beta + \gamma$ ersetzt wird, $= (\alpha, \beta + \gamma + \varepsilon) = (\alpha, \beta + \delta)$ ist, so gilt unser Satz auch für jede Combination δ vom Grade $r + 1$, also allgemein, w. z. b. w.

Satz V. Sind α, β, γ beliebige Combinationen, so ist

$$(\alpha + \gamma, \beta) = \frac{\Pi(\alpha, \beta + \gamma'')}{\Pi(\alpha, \beta + \gamma')} \tag{16}$$

wo γ'' alle paaren, γ' alle unpaaren Theile von γ durchläuft.

Den auf dieselbe Weise wie im vorigen Satze zu führenden Inductionsbeweis dürfen wir dem Leser überlassen. Als einen bemerkenswerthen speciellen Fall wollen wir aber noch den Satz

$$(\alpha, \beta) = \frac{\Pi(0, \beta + \alpha'')}{\Pi(0, \beta + \alpha')} \tag{17}$$

hervorheben, der sich aus (16) ergiebt, wenn man α, γ resp. durch 0, α ersetzt; hieraus geht nämlich hervor, dass die durch (9) definirten Elemente $(0, \omega)$ unserer Abel'schen Gruppe $\mathfrak{G}$ *unabhängige* Functionen von den willkürlich gewählten oder gegebenen Elementen $(\omega, 0)$ sind, insofern die letzteren und überhaupt alle (α, β) sich durch die ersteren ausdrücken lassen.

§. 6. Ganze Elemente in $\mathfrak{G}$.

Auch die im vorhergehenden §. 5 enthaltenen Sätze sind nur als Vorbereitungen für unser eigentliches Ziel anzusehen, welches darin besteht, die in den §§. 1 und 2 beschriebenen Zahlenbildungen so weit

wie möglich zu verallgemeinern. Zu ihrer Uebertragung auf die Abel'sche Gruppe $\mathfrak{G}$ fehlt aber bis jetzt immer noch das wesentlichste Moment, nämlich die Unterscheidung der *ganzen* und *nicht ganzen* Elemente dieser Gruppe, also auch der Begriff der *Theilbarkeit* und eine *Operation*, welche der Bildung des grössten gemeinsamen Theilers von zwei Zahlen entspricht. Der Kürze wegen beginnen wir, weil daraus alles Andere folgt, mit dem zuletzt genannten Punkte und machen die neue *Annahme*, es gebe in unserer Abel'schen Gruppe $\mathfrak{G}$ ausser der eigentlichen Gruppenoperation (der Multiplication), welche aus je zwei Elementen $\mathfrak{a}$, $\mathfrak{b}$ deren Product $\mathfrak{a}\mathfrak{b}$ erzeugt, noch eine zweite Operation $+$, die wir unbedenklich *Addition* nennen wollen, und welche aus $\mathfrak{a}$, $\mathfrak{b}$ ein Element $\mathfrak{a}+\mathfrak{b}$ derselben Gruppe $\mathfrak{G}$, die *Summe* der *Glieder* $\mathfrak{a}$, $\mathfrak{b}$ erzeugt; und zwar setzen wir voraus, dass diese Operation $+$ für sich allein und in Verbindung mit der Gruppenoperation den vier folgenden Fundamentalgesetzen

$$\mathfrak{a}+\mathfrak{a}=\mathfrak{a} \tag{1}$$
$$\mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a} \tag{2}$$
$$(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) \tag{3}$$
$$(\mathfrak{a}+\mathfrak{b})\,\mathfrak{c}=\mathfrak{a}\mathfrak{c}+\mathfrak{b}\mathfrak{c} \tag{4}$$

gehorcht, deren Inbegriff wir kurz mit G bezeichnen wollen. Diese Gesetze herrschen, wenn die Operation $+$ als Bildung des grössten gemeinsamen Theilers gedeutet wird, thatsächlich in der Theorie der rationalen Zahlen, ebenso auch in der allgemeineren Theorie der Moduln [1]), und mit gewissen Vorbehalten kann man behaupten, dass sie umgekehrt das Wesen der genannten Bildung erschöpfen.

Indem wir die aus (2) und (3) fliessenden bekannten Folgerungen übergehen (D., §. 2), bemerken wir, dass zufolge (4), wenn $\mathfrak{c}$ durch $\mathfrak{c}^{-1}$ ersetzt wird, auch die Regeln der Buchstabenrechnung für die Addition von Brüchen gelten; durch das Gesetz (1) treten aber wesentliche Vereinfachungen ein, und wir heben namentlich die beiden folgenden, leicht zu beweisenden Sätze

$$(\mathfrak{a}+\mathfrak{b}+\mathfrak{c})(\mathfrak{b}\mathfrak{c}+\mathfrak{c}\mathfrak{a}+\mathfrak{a}\mathfrak{b})=(\mathfrak{b}+\mathfrak{c})(\mathfrak{c}+\mathfrak{a})(\mathfrak{a}+\mathfrak{b}) \tag{5}$$
$$(\mathfrak{a}+\mathfrak{b})^m=\mathfrak{a}^m+\mathfrak{a}^{m-1}\mathfrak{b}+\cdots+\mathfrak{a}\mathfrak{b}^{m-1}+\mathfrak{b}^m \tag{6}$$

hervor (D., §. 170, S. 503), von denen wir sogleich Gebrauch machen werden. Multiplicirt man die rechte Seite in (6), wo $m\geqq 0$ ist, mit $(\mathfrak{a}^m+\mathfrak{b}^m)$, so wird sie $=(\mathfrak{a}+\mathfrak{b})^{2m}$, mithin ist in unserer Gruppe auch $(\mathfrak{a}+\mathfrak{b})^m=\mathfrak{a}^m+\mathfrak{b}^m$.

Vor Allem müssen wir darauf aufmerksam machen, dass durch die Annahme der Existenz der Operation $+$ innerhalb der Abel'schen

[1]) Vergl. D., §. 169, S. 496 und §. 170, S. 502. — Die Moduln $\mathfrak{a}$ bilden aber in ihrer Gesammtheit keine Abel'sche Gruppe; denn wenn es auch einen Modul $\mathfrak{o}=[1]$ giebt, welcher der Bedingung (2) in §. 5 genügt (D., §. 170, S. 500), so giebt es doch im Allgemeinen keine reciproken Moduln $\mathfrak{a}^{-1}$, welche der Bedingung (3) in §. 5 genügen.

Gruppe $\mathfrak{G}$ die Allgemeinheit der letzteren eine wesentliche *Beschränkung* erlitten hat; dies leuchtet unmittelbar ein durch den folgenden

Satz: *Die einzige in* $\mathfrak{G}$ *als Theiler enthaltene endliche Gruppe besteht aus dem Hauptelemente* $\mathfrak{o}$.

Beweis. Ist $\mathfrak{H}$ eine aus h Elementen $\mathfrak{a}$ bestehende Theilgruppe in $\mathfrak{G}$, so ist bekanntlich $\mathfrak{a}^h = \mathfrak{o}$; aus (6) ergiebt sich ferner

$$(\mathfrak{a} + \mathfrak{o})^{h-1} = \mathfrak{a}^{h-1} + \mathfrak{a}^{h-2} + \cdots + \mathfrak{a} + \mathfrak{o},$$

also

$$\mathfrak{a}(\mathfrak{a} + \mathfrak{o})^{h-1} = \mathfrak{o} + \mathfrak{a}^{h-1} + \cdots + \mathfrak{a}^2 + \mathfrak{a} = (\mathfrak{a} + \mathfrak{o})^{h-1},$$

mithin $\mathfrak{a} = \mathfrak{o}$, w. z. b. w.

Eine Abel'sche Gruppe $\mathfrak{G}$, in welcher die Operation $+$ existirt, muss daher, falls sie nicht aus einem einzigen Elemente $\mathfrak{o}$ bestehen soll — welchen interesselosen Fall wir ausschliessen wollen —, jedenfalls eine *unendliche* Gruppe sein. Eine unmittelbare Folge hiervon ist auch der

Satz: *Ist* $\mathfrak{a}$ *von* $\mathfrak{o}$ *verschieden, so folgt aus* $\mathfrak{a}^r = \mathfrak{a}^s$ *immer* $r = s$.

Beweis. Denn wenn man annimmt, es sei z. B. $r > s$, so folgt $\mathfrak{a}^{r-s} = \mathfrak{o}$, und die Potenzen $\mathfrak{o}, \mathfrak{a}, \mathfrak{a}^2 \ldots \mathfrak{a}^{r-s-1}$, mögen sie verschieden oder theilweise einander gleich sein, bilden jedenfalls eine endliche Gruppe, woraus im Widerspruch mit unserer Annahme folgen würde, dass $\mathfrak{a} = \mathfrak{o}$ ist.

Betrachten wir nun die denkbar einfachste *unendliche* Abel'sche Gruppe $\mathfrak{G}$, welche aus allen Potenzen $\mathfrak{a}^r$ eines von $\mathfrak{o}$ verschiedenen Elementes $\mathfrak{a}$ besteht, so wollen wir uns die Frage stellen: kann es in einer solchen Gruppe $\mathfrak{G}$ eine Operation $+$ geben, die den obigen Gesetzen G gehorcht? Gesetzt, es sei der Fall, so muss es eine ganze Zahl e geben, welche der Bedingung

$$\mathfrak{o} + \mathfrak{a} = \mathfrak{a}^e \tag{7}$$

genügt. Falls nun diese Zahl e *positiv* ist, so addiren wir unter Beachtung von (1) auf beiden Seiten alle Potenzen $\mathfrak{a}^r$, deren Exponenten r der Bedingung $1 \leqq r \leqq e$ genügen, und erhalten

$$\mathfrak{o} + \mathfrak{a} + \cdots + \mathfrak{a}^e = \mathfrak{a} + \cdots + \mathfrak{a}^e,$$

also

$$(\mathfrak{o} + \mathfrak{a})^e = \mathfrak{a}(\mathfrak{o} + \mathfrak{a})^{e-1}, \quad \mathfrak{o} + \mathfrak{a} = \mathfrak{a},$$

mithin muss $e = 1$ sein. Ist $m \geqq 0$, so folgt hieraus

$$\mathfrak{a}^m = (\mathfrak{o} + \mathfrak{a})^m = \mathfrak{o} + \mathfrak{a} + \cdots + \mathfrak{a}^m,$$

also zufolge (1) auch

$$\mathfrak{o} + \mathfrak{a}^m = \mathfrak{a}^m,$$

und hieraus ergiebt sich das allgemeine Gesetz

$$\mathfrak{a}^r + \mathfrak{a}^s = \mathfrak{a}^h \tag{8}$$

wo h die *algebraisch grösste* der beiden ganzen rationalen Zahlen r, s bedeutet. Sieht man umgekehrt dieses Gesetz als Definition der Opera-

tion $+$ innerhalb der Potenzengruppe $\mathfrak{G}$ an, so leuchtet ein, dass hierdurch die Gesetze G wirklich erfüllt sind. Auf ähnliche Weise lässt sich auch die zweite Annahme behandeln, dass der in (7) auftretende Exponent e *nicht positiv* ist; doch kann dieser Fall kürzer auf den vorigen zurückgeführt werden. Bedenkt man nämlich, dass unsere Gruppe $\mathfrak{G}$ auch als Inbegriff aller Potenzen des reciproken Elementes $\mathfrak{b} = \mathfrak{a}^{-1}$ aufgefasst werden kann, wodurch (7) die Form $\mathfrak{o} + \mathfrak{b} = \mathfrak{b}^{1-e}$ annimmt, so muss der nach der jetzigen Annahme *positive* Exponent $1 - e = 1$, also $e = 0$ sein, und aus dem obigen Gesetze $\mathfrak{b}^r + \mathfrak{b}^s = \mathfrak{b}^h$ ergiebt sich für diesen Fall das Gesetz

$$\mathfrak{a}^r + \mathfrak{a}^s = \mathfrak{a}^k \qquad (9)$$

wo k die *algebraisch kleinste* der Zahlen r, s bedeutet. In der aus allen Potenzen eines Elementes $\mathfrak{a}$ bestehenden unendlichen Abel'schen Gruppe $\mathfrak{G}$ giebt es daher *zwei verschiedene Operationen* $+$, deren jede zufolge ihrer Definition (8) oder (9) den vier Gesetzen G genügt.

Nachdem das Wesen dieser Gesetze durch das vorstehende Beispiel der Potenzengruppe einigermaassen erläutert ist, will ich noch zwei Beispiele von Abel'schen Gruppen $\mathfrak{G}$ anführen, in welchen es ausser der Gruppenoperation (Multiplication) auch Operationen $+$ (Additionen) giebt, welche den genannten Gesetzen gehorchen. Das System aller *Idealbrüche* $\mathfrak{a}$ eines endlichen Körpers Ω, unter denen auch die *Ideale* als *ganze* Idealbrüche enthalten sind, bildet eine Abel'sche Gruppe $\mathfrak{G}$, insofern ihre Multiplication (die Gruppenoperation) die in §. 5 angegebenen Gesetze (1), (2), (3) erfüllt (D., §. 178, S. 560, Anmerkung); ferner ist der gröfste gemeinsame Theiler $\mathfrak{a} + \mathfrak{b}$ von je zwei solchen Idealbrüchen $\mathfrak{a}$, $\mathfrak{b}$ ebenfalls in $\mathfrak{G}$ enthalten, und die hierdurch definirte Operation $+$ genügt, weil die Idealbrüche zugleich Moduln sind, auch den obigen Gesetzen G. Dieses Beispiel besitzt noch die besondere Eigenschaft, dass jedes Element $\mathfrak{a}$ der Gruppe $\mathfrak{G}$ stets und nur auf eine einzige Weise als Product von Potenzen $\mathfrak{p}^r$ darstellbar ist, deren Basen $\mathfrak{p}$ gewisse ausgezeichnete Elemente der Gruppe $\mathfrak{G}$, nämlich die *Primideale* des Körpers Ω sind, während die Exponenten r alle ganzen rationalen Zahlen durchlaufen können; um nun zu zeigen, dass diese Eigenschaft nicht etwa, wie man vermuthen könnte, den tieferen Grund für die Existenz der Operation $+$ in der Gruppe $\mathfrak{G}$ bildet, will ich noch ein *zweites* Beispiel anführen, dem die genannte Eigenschaft fehlt.

Ist a eine bestimmte von Null verschiedene *algebraische Zahl*[1]) und $\mathfrak{o}$ das System aller *algebraischen Einheiten*[2]), so bilden alle mit a *associirten* Zahlen, d. h. alle Producte von der Form ae, wo e alle Einheiten durchläuft, ein System $\mathfrak{a}$, welches ungeändert bleibt,

[1]) Vergl. S. 427, 452, 524 der zweiten, dritten, vierten Auflage von Dirichlet's Zahlentheorie.

[2]) Daselbst, S. 439, 457, 532.

wenn a selbst durch irgend eine in $\mathfrak{a}$ enthaltene Zahl ae ersetzt wird; dies beruht darauf, dass die Producte und Quotienten von irgend zwei Einheiten ebenfalls Einheiten sind. Jede in $\mathfrak{a}$ enthaltene Zahl kann daher als Repräsentant oder erzeugende Zahl von $\mathfrak{a}$ angesehen werden. Offenbar ist $\mathfrak{o}$ selbst ein solches System, als dessen Repräsentant die Zahl 1 oder jede andere Einheit gelten kann. Ist $\mathfrak{b}$ ebenfalls ein solches, durch die Zahl b erzeugtes System, so leuchtet ein, dass alle aus je einem Factor des Systems $\mathfrak{a}$ und je einem Factor des Systems $\mathfrak{b}$ gebildeten Producte dem durch das Product ab erzeugten System angehören; nennen wir dieses letztere System (dessen Zahlen umgekehrt immer, und zwar auf unendlich viele Arten als solche Producte von Zahlen aus $\mathfrak{a}$ und $\mathfrak{b}$ dargestellt werden können) das *Product* der Systeme $\mathfrak{a}$, $\mathfrak{b}$ und bezeichnen wir dasselbe mit $\mathfrak{ab}$, so bildet der Inbegriff aller dieser Systeme $\mathfrak{a}$ vermöge dieser Operation der Multiplication offenbar eine Abel'sche Gruppe $\mathfrak{G}$, deren Hauptelement das System $\mathfrak{o}$ aller Einheiten ist, während das zu $\mathfrak{a}$ reciproke Element $\mathfrak{a}^{-1}$ durch die Zahl a^{-1} erzeugt wird. Auf einem viel tiefer liegenden Grunde beruht aber die Möglichkeit, in diese Gruppe $\mathfrak{G}$ eine zweite Operation $+$ einzuführen, welche den Gesetzen G gehorcht. Ich habe bewiesen[1]), dass je zwei algebraische Zahlen a, b einen sogenannten grössten gemeinsamen Theiler d besitzen, welcher dadurch charakterisirt ist, dass es vier *ganze*[2]) algebraische Zahlen a', b', x, y giebt, welche den Bedingungen

$$a = da', \quad b = db', \quad ax + by = d \tag{10}$$

genügen; dieser Satz ist zwar nur für den damals allein wichtigen Fall bewiesen, wo a und b (also auch d) *ganze* Zahlen sind; da aber zwei beliebige algebraische Zahlen a, b durch Multiplication mit einem von Null verschiedenen Factor m stets in ganze Zahlen ma, mb verwandelt werden können[3]), so leuchtet die allgemeine Gültigkeit des Satzes sofort ein, wenn man den grössten gemeinsamen Theiler der ganzen Zahlen ma, mb mit md bezeichnet. Aus der Form der charakteristischen Gleichungen (10) ergiebt sich ferner, dass zu zwei gegebenen Zahlen a, b immer unendlich viele solche Zahlen d gehören, deren Inbegriff das in der obigen Weise durch irgend eine von ihnen erzeugte System $\mathfrak{d}$ ist, und dieses System $\mathfrak{d}$ bleibt auch ungeändert, wenn a, b durch irgend welche Zahlen der ihnen entsprechenden Systeme $\mathfrak{a}$, $\mathfrak{b}$ ersetzt werden. Das Element $\mathfrak{d}$ unserer Gruppe $\mathfrak{G}$ ist daher durch die Elemente $\mathfrak{a}$, $\mathfrak{b}$ vollständig bestimmt, und folglich wird eine neue Operation $+$ durch die Festsetzung $\mathfrak{a} + \mathfrak{b} = \mathfrak{d}$ eindeutig erklärt; dass dieselbe den

---

[1]) Vergl. S. 465, 541, 577 der zweiten, dritten, vierten Auflage von Dirichlet's Zahlentheorie.

[2]) Daselbst, S. 437, 452, 524.

[3]) Daselbst, S. 439, 493, 525.

vier Gesetzen G genügt, wird der Leser ohne Mühe aus den Gleichungen (10) ableiten. Ich bemerke aber zum Schluss, dass in dieser Gruppe $\mathfrak{G}$ eine Darstellung aller Elemente a als Producte von Potenzen von festen Primelementen *nicht* vorhanden ist (vergl. D., §. 174). —

Wir verlassen diese Beispiele und wenden uns zur Betrachtung irgend einer Abel'schen Gruppe $\mathfrak{G}$, in welcher es eine Addition $+$ mit den obigen Eigenschaften giebt. Indem wir nun eine Reihe von Benennungen einführen, die denen der Zahlentheorie nachgebildet sind, bemerken wir vor allen Dingen, dass dieselben sich stets auf diese eine Operation $+$ beziehen; dies muss deshalb hervorgehoben werden, weil es, wie sich bald zeigen wird, in jeder solchen Gruppe $\mathfrak{G}$ mindestens *zwei verschiedene* solche Operationen $+$ giebt (vergl. das obige Beispiel der aus allen Potenzen a^r bestehenden Gruppe auf S. 24).

Wir nennen ein Element a der Gruppe $\mathfrak{G}$ *ganz*, wenn $a + o = o$ ist, im entgegengesetzten Falle *gebrochen*. Dann ergiebt sich zunächst, dass alle Producte und Summen von ganzen Elementen ebenfalls ganz sind; denn durch Addition der beiden Gleichungen $a + o = o$, $b + o = o$ erhält man $(a + b) + o = o$; multiplicirt man ferner die erste mit b, so folgt $ab + b = b$, und wenn man auf beiden Seiten o addirt, so ergiebt sich $ab + o = o$, w. z. b. w.

Das (ganze oder gebrochene) Element a soll *theilbar* durch b heissen, wenn $a + b = b$ ist; dies kommt offenbar darauf hinaus, dass ab^{-1} ein *ganzes* Element g, also $a = bg$ ist; wir nennen zugleich a ein *Vielfaches* von b, und b einen *Theiler* von a, und es leuchtet ein, dass die durch das Hauptelement o theilbaren Elemente, und nur diese ganz sind. Benutzt man (wie in der Modultheorie) für diese Theilbarkeit die doppelte Bezeichnung

$$a > b, \quad b < a,$$

so findet man leicht, dass aus $a > b$ und $b > c$ auch $a > c$, und dass aus $a > b$ und $b > a$ auch $a = b$ folgt.

Die Summe $a + b$ von zwei beliebigen Elementen a, b ist immer ein gemeinsamer Theiler derselben, und jeder gemeinsame Theiler n von a, b ist ein Theiler von der Summe $a + b$, weil aus $a + n = n$ und $b + n = n$ durch Addition auch $(a + b) + n = n$ folgt; der Analogie wegen kann man daher die Summe $a + b$ auch den *grössten* gemeinsamen Theiler von a, b nennen.

Zwei Elemente a, b sollen *fremd*[1]) heissen, wenn ihre Summe $a + b = o$ ist; zwei solche Elemente a, b sind offenbar stets *ganze* Elemente, und o ist ihr einziger *ganzer* gemeinsamer Theiler.

---

[1]) Dieses Wort wird hier in ganz anderem Sinne gebraucht, wie bei den Combinationen in §. 3, nämlich analog dem Begriffe der relativen Primzahlen in der Zahlentheorie.

Ist a fremd zu b und zu c, so ist a auch fremd zu bc; multiplicirt man nämlich die erste der beiden Gleichungen $a + b = o$, $a + c = o$, aus deren letzter auch $c + o = o$, also $ac + a = a$ folgt, mit c, so erhält man $ac + bc = c$, und wenn man auf beiden Seiten a addirt, so folgt $(a + ac) + bc = a + c$, also $a + bc = o$, w. z. b. w.

Umgekehrt, wenn a fremd zu dem Producte bc der beiden *ganzen* Elemente b, c ist, so ist a auch fremd zu jedem der beiden Factoren b, c; denn aus der letzten der drei Annahmen $a + bc = o$, $b + o = o$, $c + o = o$ folgt $b = bc + b$, also $a + b = (a + bc) + b = o + b = o$, w. z. b. w.

Durch wiederholte Anwendung dieser beiden Sätze ergiebt sich der allgemeinere: zwei Producte p, q sind gewiss fremd, wenn jeder Factor von p fremd zu jedem Factor von q ist, und umgekehrt folgt das Letztere auch aus dem Ersteren, wenn zugleich alle diese Factoren ganz sind.

Sind a, b beliebige Elemente, so sind die aus ihnen gebildeten Elemente

$$a' = \frac{a}{a + b}, \quad b' = \frac{b}{a + b}$$

immer fremd, d. h. es ist $a' + b' = o$; man kann daher

$$a = (a + b)a', \qquad b = (a + b)b'$$

setzen, und jeder Quotient $(a : b)$, also auch jedes Element $a = (a : o)$, kann folglich in der Form $(a' : b')$, d. h. als Quotient von zwei fremden Elementen a', b' dargestellt werden; dass es nur eine einzige solche Darstellung giebt, ist leicht zu beweisen.

Indem wir eine Reihe anderer, ebenso leicht zu beweisender Sätze über fremde Elemente übergehen, wenden wir uns zur Betrachtung der *gemeinsamen Vielfachen* c von zwei Elementen a, b, wobei wir die eben festgesetzte Bedeutung von a', b' beibehalten. Aus den Annahmen $c + a = a$, $c + b = b$ folgt durch Multiplication mit b, a resp. $bc + ab = ab$, $ac + ab = ab$, und hieraus durch Addition $(a + b)c + ab = ab$, oder wenn man durch $(a + b)$ dividirt und

$$m = \frac{ab}{a + b} = ab' = ba' = (a + b)\,a'b'$$

setzt, $c + m = m$, d. h. c ist theilbar durch m; da nun fremde Elemente a', b' stets ganz sind, so ist m ebenfalls theilbar durch a und b, mithin sind die gemeinsamen Vielfachen c von a, b identisch mit den sämmtlichen Vielfachen dieses Elementes m, welches daher nach Analogie mit der Zahlentheorie das *kleinste* gemeinsame Vielfache von a, b heissen mag. Wir wollen nun die Bildung dieses Elementes m aus den Elementen a, b als eine neue *Operation* — in unsere Gruppe einführen; dieselbe wird also definirt durch

$$a - b = \frac{ab}{a + b} \tag{11}$$

oder, was dasselbe sagt, durch

$$a - b = (a^{-1} + b^{-1})^{-1} \tag{12}$$

und zugleich gilt der Satz

$$(a + b)(a - b) = ab \tag{13}$$

Vor Allem bemerken wir, dass diese neue Operation — für sich allein und in Verbindung mit der Gruppenoperation den vier folgenden Gesetzen

$$a - a = a \tag{1'}$$
$$a - b = b - a \tag{2'}$$
$$(a - b) - c = a - (b - c) \tag{3'}$$
$$(a - b)c = ac - bc \tag{4'}$$

gehorcht, welche vollständig den Gesetzen G entsprechen, und deren Inbegriff wir mit G' bezeichnen wollen. Die Beweise von (1') und (2') liegen auf der Hand. Ferner ergiebt sich aus der Definition

$$(a - b) - c = \frac{(a - b)c}{(a - b) + c}$$

und wenn man den Bruch rechter Hand unter Beachtung von (13) durch $(a + b)$ erweitert, so erhält man

$$(a - b) - c = \frac{abc}{bc + ca + ab} = (a^{-1} + b^{-1} + c^{-1})^{-1},$$

woraus wegen der Symmetrie (3') folgt. Ebenso ergiebt sich die Gleichung (4'), weil jede ihrer beiden Seiten, wenn sie mit $(a + b)\,c = (ac + bc)$ multiplicirt wird, dasselbe Product abc^2 giebt.

Es erscheint also hier die schon oben angekündigte merkwürdige Thatsache, dass, wenn es in einer Abel'schen Gruppe $\mathfrak{G}$ eine Operation $+$ giebt, welche den Gesetzen G gehorcht, daraus immer eine zweite Operation $-$ abgeleitet werden kann, welche genau dieselben Gesetze befolgt. Es fragt sich daher: können diese beiden Operationen $\pm$ vielleicht identisch sein? Nehmen wir an, zwei Elemente a, b genügen der Bedingung $a - b = a + b$, woraus durch Multiplication mit $(a + b)$ auch $ab = (a + b)^2 = a^2 + ab + b^2$ folgt, so erhält man durch Addition von a^2 und von b^2 die beiden Gleichungen $a(a + b) = (a + b)^2$ und $b(a + b) = (a + b)^2$, mithin $a = b = a + b$; da also für je zwei *verschiedene* Elemente a, b auch $(a - b)$ verschieden von $(a + b)$ wird, so sind die beiden Operationen $\pm$ *nicht* identisch mit einander; aus (12) geht aber zugleich hervor, dass sie sich vollständig mit einander vertauschen, wenn jedes Element a der Gruppe $\mathfrak{G}$ durch das reciproke Element a^{-1} ersetzt wird (vergl. das oben angeführte Beispiel der einfachen Potenzengruppe). Hierbei wollen wir auch bemerken, dass der Satz (12), auf eine beliebige Anzahl von Elementen ausgedehnt, in der doppelten Form [1])

[1]) Vergl. D., §. 178, S. 555.

$$(a - b - c - \cdots)^{-1} = a^{-1} + b^{-1} + c^{-1} + \cdots \quad (14)$$
$$(a + b + c + \cdots)^{-1} = a^{-1} - b^{-1} - c^{-1} - \cdots \quad (15)$$

dargestellt werden kann, was durch vollständige Induction leicht zu beweisen ist.

Es erscheint ferner die andere merkwürdige Thatsache, dass zwischen den beiden Operationen $\pm$ auch die Beziehungen

$$a + (a - b) = a \quad (16)$$
$$a - (a + b) = a \quad (17)$$

bestehen, welche schon daraus folgen, dass $a - b$ durch a, und a durch $a + b$ theilbar ist; man kann sie aber auch dadurch beweisen, dass man die linke Seite der ersten Gleichung mit $(a + b)$, die der zweiten mit $(a - b)$ multiplicirt, wodurch zufolge (13) resp. die Producte $a(a + b)$, $a(a - b)$ entstehen. Offenbar stimmen nun die sechs Gesetze (2), (3), (2′), (3′), (16), (17), in welchen die eigentliche Gruppenoperation gar nicht auftritt, genau mit den sechs Gesetzen A des §. 3 überein, welche dann die Grundlage für die Betrachtungen des §. 4 gebildet haben; wir können daher sagen, dass unsere Abel'sche Gruppe $\mathfrak{G}$, wenn man von der Multiplication ihrer Elemente ganz absieht und nur die beiden Operationen $\pm$ in das Auge fasst, auch eine *Dualgruppe* ist, und wir wollen zum Schluss noch zeigen, dass dieselbe den *Idealtypus* besitzt, d. h. dass in ihr das Doppelgesetz (5) des §. 3 gilt:

$$(a - b) + (a - c) = a - (b + c) \quad (18)$$
$$(a + b) - (a + c) = a + (b - c) \quad (19)$$

Dies ergiebt sich aus der Definition der Operation — durch die folgenden Rechnungen:

$$(a - b) + (a - c) = \frac{ab}{a + b} + \frac{ac}{a + c} = \frac{a(bc + ca + ab)}{(a + b)(c + a)}$$
$$a - (b + c) = \frac{a(b + c)}{a + b + c}$$
$$(a + b) - (a + c) = \frac{(a + b)(c + a)}{a + b + c}$$
$$a + (b - c) = a + \frac{bc}{b + c} = \frac{bc + ca + ab}{b + c}$$

und aus dem obigen Satze (5) folgt die Identität der beiden ersten und ebenso die der beiden letzten Ausdrücke, w. z. b. w.

§. 7. Lösung der Aufgabe.

Wir kehren jetzt zurück zu der in §§. 1 und 2 für rationale Zahlen behandelten Aufgabe, um dieselbe auf ein beliebig gegebenes System von n Elementen

$$a_1, a_2 \ldots a_n \quad (1)$$

der in den §§. 5 und 6 betrachteten Abel'schen Gruppe $\mathfrak{G}$ zu übertragen. Es handelt sich darum, diejenigen Zerlegungen dieser Elemente in Factoren zu finden, welche sich aus der Bildung der grössten gemeinsamen Theiler

$$\begin{array}{l} a_1 + a_2, \quad a_1 + a_3 \ldots \\ a_1 + a_2 + a_3, \quad a_1 + a_2 + a_4 \ldots \\ a_1 + a_2 + a_3 + a_4 \ldots \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{array}$$

von irgend welchen Combinationen aus diesen Elementen ableiten lassen; diese grössten gemeinsamen Theiler sind, da ihre Bildung als stets ausführbar angenommen wird, ebenfalls als gegeben anzusehen.

Zu diesem Zwecke benutzen wir die in §. 5 beschriebene Bezeichnungsweise, indem wir zunächst die n *gegebenen* Elemente (1) der Reihe nach mit den Zeichen

$$(1,0), (2,0) \ldots (n, 0) \tag{2}$$

belegen. Während nun in §. 5 auch alle anderen Elemente von der Form $(\alpha, 0)$, wo α jede beliebige Combination aus den n Unterscheidungszeichen $1, 2 \ldots n$ bedeutet, als *willkürlich* wählbar oder gegeben angesehen werden durften, so wollen wir jetzt diese Wahlfreiheit gänzlich aufheben, indem wir festsetzen, dass

$$(\alpha, 0) = (\varepsilon_1, 0) + (\varepsilon_2, 0) + \cdots \tag{3}$$

sein soll, wo $\varepsilon_1, \varepsilon_2 \ldots$ die sämmtlichen Combinationen *ersten* Grades bedeuten, deren Summe die Combination α ist; es wird also $(\alpha, 0)$ definirt als der grösste gemeinsame Theiler aller derjenigen in der Reihe (2) enthaltenen Gruppenelemente $(\varepsilon, 0)$, welche den in α enthaltenen Combinationselementen ε entsprechen; falls α selbst vom ersten Grade ist, so besteht die Summe (3) aus einem einzigen Gliede, welches das entsprechende Element in der Reihe (2) ist. Hiermit sind alle Elemente $(\alpha, 0)$ durch (2) vollständig *gegeben*, mit Ausnahme des Elementes (0,0), das vorläufig noch *willkürlich* bleiben mag.

Aus diesen Elementen $(\alpha, 0)$, deren Anzahl $= 2^n$ ist, bilden wir nun nach der Definition (9) in §. 5, also durch Multiplication und Division, alle Elemente von der Form (α, β); diese sind daher, *wenn α von 0 verschieden ist*, ebenfalls durch die n Elemente (2) vollständig *gegeben*, während in allen Ausdrücken von der Form $(0, \beta)$ auch das Element (0, 0) auftritt. Dann gelten die in §. 5 bewiesenen Sätze I bis V, und von diesen giebt der allgemeine *Productsatz III* die *vollständige Lösung unserer Aufgabe.* Die Beschaffenheit dieser Lösung wollen wir aber durch die folgenden Sätze deutlich machen, welche aus der Definition (3) fliessen.

Satz I. Sind die Combinationen α, β von 0 verschieden und ω beliebig, so ist

$$(\alpha, \omega) + (\beta, \omega) = (\alpha + \beta, \omega) \tag{4}$$

Beweis. Zunächst leuchtet ein, dass dieser Satz für $\omega = 0$ gilt. Denn wenn ε alle Elemente der Combination α, ebenso η alle Elemente der Combination β durchläuft, so ist $(\alpha, 0)$ zufolge (3) die Summe aller $(\varepsilon, 0)$, ebenso ist $(\beta, 0)$ die Summe aller $(\eta, 0)$, und $(\alpha + \beta, 0)$ ist die Summe aller $(\theta, 0)$, wo θ alle Elemente der Combination $(\alpha + \beta)$ durchläuft. Nun tritt zwar, wenn α und β gemeinsame Elemente $\varepsilon = \eta$ besitzen, das Glied $(\varepsilon, 0) = (\eta, 0)$ auf der linken Seite der zu beweisenden Gleichung (4) sowohl in der Summe $(\alpha, 0)$, wie in der Summe $(\beta, 0)$ auf, allein zufolge des Satzes $\mathfrak{a} + \mathfrak{a} = \mathfrak{a}$ braucht ein solches Glied nur einmal gezählt zu werden, und da die Elemente von α und die von β zugleich alle Elemente θ der Summe $(\alpha + \beta)$ erschöpfen, so ergiebt sich die Wahrheit des Satzes für diesen Fall $\omega = 0$. Wir nehmen nun an, der Satz sei für alle Combinationen ω vom Grade r bewiesen, und wollen zeigen, dass er dann (falls $r < n$ ist) auch für jede Combination vom Grade $(r + 1)$ gilt. Jede solche Combination lässt sich in die Form $\omega + \varepsilon$ setzen, wo ε jetzt irgend eine Combination ersten Grades bedeutet, welche in der Combination ω vom Grade r nicht enthalten ist. Setzen wir ferner zur Abkürzung

$$(\alpha, \omega) = \mathfrak{a}, \quad (\beta, \omega) = \mathfrak{b}, \quad (\varepsilon, \omega) = \mathfrak{c},$$

so folgt aus unserer Inductionshypothese

$$(\alpha + \varepsilon, \omega) = \mathfrak{a} + \mathfrak{c}, \qquad (\beta + \varepsilon, \omega) = \mathfrak{b} + \mathfrak{c},$$
$$(\alpha + \beta, \omega) = \mathfrak{a} + \mathfrak{b}, \quad (\alpha + \beta + \varepsilon, \omega) = \mathfrak{a} + \mathfrak{b} + \mathfrak{c},$$

und aus dem speciellen Productsatz II in §. 5 ergiebt sich:

$$\mathfrak{a} = (\mathfrak{a} + \mathfrak{c})(\alpha, \omega + \varepsilon), \quad \mathfrak{b} = (\mathfrak{b} + \mathfrak{c})(\beta, \omega + \varepsilon),$$
$$\mathfrak{a} + \mathfrak{b} = (\mathfrak{a} + \mathfrak{b} + \mathfrak{c})(\alpha + \beta, \omega + \varepsilon).$$

Hieraus folgt weiter

$$(\mathfrak{a} + \mathfrak{c})(\mathfrak{b} + \mathfrak{c})\{(\alpha, \omega + \varepsilon) + (\beta, \omega + \varepsilon)\} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) + \mathfrak{b}(\mathfrak{a} + \mathfrak{c})$$
$$= \mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b};$$

multiplicirt man diese Gleichung mit der vorhergehenden und dividirt man die Productgleichung durch die Gleichung (5) in §. 6, nämlich durch

$$(\mathfrak{b} + \mathfrak{c})(\mathfrak{c} + \mathfrak{a})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b} + \mathfrak{c})(\mathfrak{b}\mathfrak{c} + \mathfrak{c}\mathfrak{a} + \mathfrak{a}\mathfrak{b}),$$

so erhält man

$$(\alpha, \omega + \varepsilon) + (\beta, \omega + \varepsilon) = (\alpha + \beta, \omega + \varepsilon),$$

d. h. unser Satz gilt auch für jede Combination $(\omega + \varepsilon)$ vom Grade $(r + 1)$, also allgemein, w. z. b. w.

Satz II. Sind die Combinationen α, β von 0 verschieden, so ist (α, β) ein ganzes Element der Gruppe $\mathfrak{G}$.

Beweis. Ist β von 0 verschieden, so sind die Elemente (β, β) und $(\alpha + \beta, \beta)$ nach Satz I in §. 5 beide $= \mathfrak{o}$, und da, wenn α ebenfalls von 0 verschieden ist, nach dem eben bewiesenen Satze $(\alpha, \beta) + (\beta, \beta) = (\alpha + \beta, \beta)$ ist, so ergiebt sich $(\alpha, \beta) + \mathfrak{o} = \mathfrak{o}$, w. z. b. w.

Satz III. Genügen die vier Combinationen $\alpha, \beta, \gamma, \delta$ *der Bedingung* $\alpha + \beta = \gamma + \delta$, *und sind ausserdem die Durchschnitte* $\alpha - \delta$ *und* $\beta - \gamma$ *beide von* 0 *verschieden, so sind* (α, β) *und* (γ, δ) *fremde Elemente, in Zeichen*

$$(\alpha, \beta) + (\gamma, \delta) = 0 \tag{5}$$

Beweis. Wenn die Bedingung $\alpha + \beta = \gamma + \delta$ erfüllt ist, so wird nach einem in §. 3 bewiesenen Satze (S. 10)

$$\beta = \varrho + \omega, \quad \delta = \sigma + \omega$$
$$\alpha + \varrho = \gamma + \sigma = \alpha + \gamma,$$

wo zur Abkürzung

$$\beta - \gamma = \varrho, \quad \alpha - \delta = \sigma, \quad \beta - \delta = \omega$$

gesetzt ist. Wir wenden jetzt den allgemeinen Productsatz III des §. 5 auf die beiden Elemente (α, ω), (γ, ω) an, indem wir die dort mit γ bezeichnete Combination einmal durch ϱ, das andere Mal durch σ ersetzen; in den so erhaltenen Gleichungen

$$(\alpha, \omega) = \Pi(\alpha + \varrho_1, \omega + \varrho_2)$$
$$(\gamma, \omega) = \Pi(\gamma + \sigma_1, \omega + \sigma_2)$$

bezieht sich das erste Productzeichen auf alle Zerlegungen $\varrho = \varrho_1 + \varrho_2$ mit der Bedingung $\varrho_1 - \varrho_2 = 0$, das zweite auf alle Zerlegungen $\sigma = \sigma_1 + \sigma_2$ mit der Bedingung $\sigma_1 - \sigma_2 = 0$. Da nun nach unserer Annahme die beiden Durchschnitte ϱ, σ (also auch $\alpha, \beta, \gamma, \delta$) von 0 verschieden sind, so besteht jedes dieser beiden Producte aus mindestens zwei Factoren, und zwar sind die Factoren $(\alpha + \varrho, \omega)$ und $(\gamma + \sigma, \omega)$, welche den Zerlegungen $\varrho_1 = \varrho$, $\varrho_2 = 0$ und $\sigma_1 = \sigma$, $\sigma_2 = 0$ entsprechen, identisch mit $(\alpha + \gamma, \omega)$; bezeichnen wir daher die Producte aller *übrigen* Factoren resp. mit $\mathfrak{p}$ und $\mathfrak{q}$, so wird

$$(\alpha, \omega) = (\alpha + \gamma, \omega)\mathfrak{p}, \quad (\gamma, \omega) = (\alpha + \gamma, \omega)\mathfrak{q};$$

da ferner, wie schon bemerkt, auch α, γ von 0 verschieden sind, so ist $(\alpha + \gamma, \omega)$ nach Satz I die Summe der beiden vorstehenden Elemente, mithin

$$\mathfrak{p} + \mathfrak{q} = 0,$$

d. h. die genannten Producte $\mathfrak{p}$, $\mathfrak{q}$ sind *fremd* zu einander. Nun war $\mathfrak{p}$ das Product aus allen denjenigen Factoren $(\alpha + \varrho_1, \omega + \varrho_2)$, in welchen ϱ_2 von 0 verschieden ist, und da Letzteres auch von α, also auch von $\alpha + \varrho_1$ und $\omega + \varrho_2$ gilt, so ist (nach Satz II) jeder solche Factor $(\alpha + \varrho_1, \omega + \varrho_2)$ ein *ganzes* Element der Gruppe, und dasselbe gilt offenbar von jedem Factor $(\gamma + \sigma_1, \omega + \sigma_2)$ des Productes $\mathfrak{q}$, weil γ und σ_2, also auch $\gamma + \sigma_1$ und $\omega + \sigma_2$, von 0 verschieden sind. Da aber das Product $\mathfrak{p}$ der ganzen Factoren $(\alpha + \varrho_1, \omega + \varrho_2)$, wie oben gezeigt ist, fremd zu dem Producte $\mathfrak{q}$ der ganzen Factoren $(\gamma + \sigma_1, \omega + \sigma_2)$ ist, so folgt nach einem in §. 6 bewiesenen Satze (S. 28), dass auch jeder der Factoren von $\mathfrak{p}$ fremd zu jedem der

Factoren von $\mathfrak{q}$ ist; unter den ersteren befindet sich aber der der Zerlegung $\varrho_1 = 0$, $\varrho_2 = \varrho$ entsprechende Factor $(\alpha, \omega + \varrho) = (\alpha, \beta)$, und unter den letzteren befindet sich der der Zerlegung $\sigma_1 = 0$, $\sigma_2 = \sigma$ entsprechende Factor $(\gamma, \omega + \sigma) = (\gamma, \delta)$; mithin ist (α, β) fremd zu (γ, δ), w. z. b. w.

Satz IV. Sind die Combinationen α, β von 0 verschieden und ω beliebig, so ist

$$(\omega, \alpha) + (\omega, \beta) = (\omega, \alpha + \beta) \tag{6}$$

Beweis. Nach dem allgemeinen Productsatze III des §. 5 können wir

$$(\omega, \alpha) = \Pi(\omega + \beta_1, \quad \alpha + \beta_2)$$
$$(\omega, \beta) = \Pi(\omega + \alpha_1, \quad \beta + \alpha_2)$$

setzen, wo sich das erste Productzeichen auf alle Zerlegungen $\beta = \beta_1 + \beta_2$ mit der Bedingung $\beta_1 - \beta_2 = 0$, das zweite auf alle Zerlegungen $\alpha = \alpha_1 + \alpha_2$ mit der Bedingung $\alpha_1 - \alpha_2 = 0$ bezieht. Da α, β nach unserer Annahme von 0 verschieden sind, so besteht jedes dieser beiden Producte aus mindestens zwei Factoren, und zwar sind die den beiden Zerlegungen $\beta_1 = 0$, $\beta_2 = \beta$ und $\alpha_1 = 0$, $\alpha_2 = \alpha$ entsprechenden Factoren identisch mit $(\omega, \alpha + \beta)$; bezeichnen wir daher die Producte aller *übrigen* Factoren resp. mit $\mathfrak{p}$ und $\mathfrak{q}$, so wird

$$(\omega, \alpha) = (\omega, \alpha + \beta)\,\mathfrak{p}, \quad (\omega, \beta) = (\omega, \alpha + \beta)\,\mathfrak{q}.$$

Vergleichen wir nun irgend einen Factor $(\omega + \beta_1, \alpha + \beta_2)$ von $\mathfrak{p}$ mit irgend einem Factor $(\omega + \alpha_1, \beta + \alpha_2)$ von $\mathfrak{q}$, so genügen die vier in ihnen auftretenden Combinationen zunächst der Bedingung

$$(\omega + \beta_1) + (\alpha + \beta_2) = (\omega + \alpha_1) + (\beta + \alpha_2),$$

weil jede dieser beiden Summen $= \omega + \alpha + \beta$ ist; da ferner β_1 ein von 0 verschiedener Theil von β, und α_1 ein von 0 verschiedener Theil von α ist, so sind auch die Durchschnitte

$$(\omega + \beta_1) - (\beta + \alpha_2), \quad (\omega + \alpha_1) - (\alpha + \beta_2)$$

beide von 0 verschieden. Aus diesen Eigenschaften der vier Combinationen folgt aber (nach Satz III), dass jeder Factor $(\omega + \beta_1, \alpha + \beta_2)$ von $\mathfrak{p}$ fremd zu jedem Factor $(\omega + \alpha_1, \beta + \alpha_2)$ von $\mathfrak{q}$ ist; nach einem in §. 6 bewiesenen Satze (S. 28) ist daher auch $\mathfrak{p}$ fremd zu $\mathfrak{q}$, also

$$\mathfrak{p} + \mathfrak{q} = \mathfrak{o}$$

und hieraus folgt durch Addition der beiden letzten Darstellungen von (ω, α) und (ω, β) die Gleichung (6), w. z. b. w.

Satz V. Ist die Combination α von 0 verschieden, ω beliebig, so ist (ω, α) die Summe aller (ω, ε), wo ε alle in α enthaltenen Combinationen ersten Grades durchläuft.

Dies ist offenbar eine unmittelbare Folge des vorhergehenden Satzes IV. Vergleicht man den speciellen Fall $\omega = 0$ mit der obigen Definition (3) der Elemente $(\alpha, 0)$, so zeigt sich, dass die schon am

Schluss von §. 5 hervorgehobene Analogie zwischen den Elementen $(\alpha, 0)$ und $(0, \alpha)$ auch nach unseren jetzigen Beschränkungen hinsichtlich der Wahl dieser Elemente bestehen bleibt.

Satz VI. Ist die Combination α von 0 verschieden, ω beliebig, so ist der Quotient

$$\frac{(\omega, 0)}{(\omega, \alpha)} \tag{7}$$

das kleinste gemeinsame Vielfache aller Elemente $(\omega + \varepsilon, 0)$, wo ε alle in α enthaltenen Combinationen ersten Grades $\varepsilon_1, \varepsilon_2 \ldots$ durchläuft.

Beweis. Nach dem speciellen Productsatze (10) des §. 5 ist $(\omega, 0) = (\omega + \varepsilon, 0)(\omega, \varepsilon)$, also

$$(\omega, 0)(\omega + \varepsilon, 0)^{-1} = (\omega, \varepsilon).$$

Bezeichnet man nun das im Satze genannte kleinste gemeinsame Vielfache

$$(\omega + \varepsilon_1, 0) - (\omega + \varepsilon_2, 0) - \cdots$$

zur Abkürzung mit $\mathfrak{m}$, und wendet man den Satz (14) des §. 6 an, so folgt

$$\mathfrak{m}^{-1} = (\omega + \varepsilon_1, 0)^{-1} + (\omega + \varepsilon_2, 0)^{-1} + \cdots,$$

also

$$(\omega, 0)\,\mathfrak{m}^{-1} = (\omega, \varepsilon_1) + (\omega, \varepsilon_2) + \cdots,$$

und da nach dem vorhergehenden Satze V diese Summe $= (\omega, \alpha)$ ist, so ergiebt sich

$$(\omega, 0)\,\mathfrak{m}^{-1} = (\omega, \alpha), \quad \mathfrak{m} = \frac{(\omega, 0)}{(\omega, \alpha)},$$

w. z. b. w. —

Hiermit sind wohl die wichtigsten Eigenschaften der Ausdrücke (α, β) erschöpft, welche zuerst in §. 5 durch die Gleichung (9) eingeführt, jetzt aber durch die Definition (3) sämmtlich auf die n gegebenen Elemente (2) und, falls $\alpha = 0$ ist, auf (0,0) zurückgeführt sind. Von diesen Ausdrücken (α, β), deren Anzahl $= 4^n$ ist, bieten diejenigen, in welchen $\alpha - \beta$ von 0 verschieden ist, gar kein Interesse dar, weil sie nach Satz I in §. 5 alle $= 0$ sind; wir wollen daher nur noch die übrigen betrachten, in denen $\alpha - \beta = 0$, und deren Anzahl $= 3^n$ ist. Von diesen wollen wir vorläufig auch alle diejenigen *ausschliessen*, in denen $\alpha = 0$ ist, also nur solche Elemente (α, β) beibehalten, die durch das System (2) ohne Zuziehung des Elementes (0, 0) gegeben sind. Bezeichnen wir nun mit ν immer die aus allen n Zeichen $1, 2 \ldots n$ bestehende Combination, und nennen wir jedes Element (ν_1, ν_2), welches der Bedingung $\nu_1 + \nu_2 = \nu$ genügt, einen *Kern* (sc. des in (2) gegebenen Systems), so ergiebt sich aus dem allgemeinen Productsatze III des §. 5, dass jedes andere Element (α, β) als ein *Product von lauter Kernen* darstellbar ist; wählt man nämlich dort für γ diejenige Combination, welche aus allen in $(\alpha + \beta)$ fehlenden

Combinationselementen besteht, so leuchtet ein, dass alle Factoren des Productes

$$(\alpha, \beta) = \Pi(\alpha + \gamma_1, \beta + \gamma_2) \tag{8}$$

Kerne sind, weil $(\alpha + \gamma_1) + (\beta + \gamma_2) = \alpha + \beta + \gamma = \nu$ ist. Die Anzahl aller Kerne (zu denen $(0, \nu)$ nicht gehört) ist $= 2^n - 1$, und wenn a, b, c die Grade der Combinationen α, β, γ bedeuten, so ist $a + b + c = n$, und 2^c ist die Anzahl aller Kernfactoren von (α, β). Von besonderer Wichtigkeit für diese Darstellungen, unter denen sich offenbar auch die in der Ueberschrift dieses Aufsatzes genannten Zerlegungen der n gegebenen Elemente (2) befinden, ist ferner unser obiger Satz III, weil er lehrt, wann zwei Kerne *gewiss* zu einander *fremd* sind. Für den Fall $n = 4$ geben die Gleichungen (3), (5), (7) des §. 2 die Kernzerlegungen der Elemente $(\alpha, 0)$; die übrigen Elemente (α, β) und ihre Zerlegungen, wie z. B.

$$(1,2) = (134,2)\,(13,24)\,(14,23)\,(1,234)$$

sind damals absichtlich gar nicht erwähnt, um die Aufmerksamkeit nicht von der Hauptsache, der Herstellung der Zerlegungen (7), abzulenken. Schliesslich ist zu bemerken, dass zufolge des obigen Satzes II alle Kerne mit Ausnahme von $(\nu, 0)$ gewiss *ganze* Elemente der Gruppe $\mathfrak{G}$ sind, was für $(\nu, 0)$ dann und nur dann gilt, wenn die gegebenen Elemente (2) sämmtlich ganz sind. —

Nun noch einige Worte über die Bedeutung der Elemente von der Form $(0, \alpha)$! Sie lässt sich am einfachsten aussprechen, wenn man für das bisher willkürliche Element $(0, 0)$ das *Hauptelement* $\mathfrak{o}$ der Gruppe $\mathfrak{G}$ wählt. Aus dem Satze VI geht dann, wenn $\omega = 0$ gesetzt wird, das specielle, der Definition (3) dualistisch entsprechende Resultat hervor, dass $(0, \alpha)^{-1}$ das kleinste gemeinsame Vielfache aller Elemente $(\varepsilon, 0)$ ist, wo ε alle in α enthaltenen Combinationen ersten Grades durchläuft. Wendet man aber auch auf diese Elemente $(0, \alpha)$ die Zerlegung (8) an, so ergiebt sich

$$\mathfrak{o} = (0, 0) = \Pi(\nu_1, \nu_2), \quad (0, \alpha) = \Pi(\gamma_1, \alpha + \gamma_2);$$

in der ersten dieser beiden Formeln findet sich das *Product aller Kerne* multiplicirt mit $(0, \nu)$, und folglich ist dieses Product das kleinste gemeinsame Vielfache aller n Elemente (2); auch die Factoren des zweiten Productes sind mit Ausnahme von $(0, \nu)$ lauter Kerne, und wenn man die erste Gleichung durch die zweite dividirt, so stellt sich auch das oben genannte kleinste gemeinsame Vielfache $(0, \alpha)^{-1}$ als Product von lauter Kernen dar, worauf wir aber hier nicht weiter eingehen wollen.

§. 8. Endliche Dualgruppen in $\mathfrak{G}$.

Wir wollen zum Schluss noch eine Anwendung von den besprochenen Zerlegungen machen. In §. 6 ist gezeigt, dass die Abel'sche Gruppe $\mathfrak{G}_\nu$ wenn es ausser der Gruppenoperation (Multiplication) in ihr noch

eine Addition $+$ giebt, welche den dort angegebenen Gesetzen G gehorcht, keine *endliche* Gruppe (ausser 0) als Theiler enthalten kann, wobei natürlich als Operation der Theilgruppe dieselbe Multiplication angesehen wurde. Dieselbe Gruppe $\mathfrak{G}$ besitzt nun aber in Bezug auf die beiden Operationen $\pm$ auch den Charakter einer *Dualgruppe* vom *Idealtypus*, und sie kann, so aufgefasst, sehr wohl *endliche Dualgruppen* als Theiler enthalten. Nehmen wir wie in §. 7 an, es sei ein System von n Elementen

$$(1,0), (2,0) \ldots (n, 0) \tag{1}$$

der Gruppe $\mathfrak{G}$ gegeben, und bilden wir aus ihnen durch stets wiederholte Anwendung beider Operationen $\pm$ immer neue Elemente, welche dem gegebenen System hinzugefügt werden, so wird, wie wir beweisen wollen, diese Bildung nach einer endlichen Anzahl von Schritten ihr Ende finden, insofern die Operationen $\pm$ aus je zwei Elementen, welche in dem so entstandenen System $\mathfrak{P}$ enthalten sind, nur noch solche Elemente erzeugen, welche schon in $\mathfrak{P}$ enthalten sind. Zugleich wird sich ergeben, dass alle Elemente dieser endlichen Dualgruppe $\mathfrak{P}$ sich durch die in §. 7 betrachteten *Kerne* des Systems (1) ausdrücken lassen. Am kürzesten gelangt man *synthetisch* zum Ziele, indem man umgekehrt von der gemeinsamen Form dieser Ausdrücke ausgeht, deren Auffindung mir erst nach längerem Nachdenken gelungen ist.

Ich erinnere zunächst an die, in der Gleichung (8) des §. 7 enthaltene Darstellung jedes Elementes von der Form $(\alpha, 0)$, wo α, wie immer im Folgenden, von 0 verschieden sein soll, als Product von lauter Kernen; stellt man die Combination β, welche aus allen in α fehlenden Elementen besteht, auf alle verschiedenen Arten als Summe $\beta_1 + \beta_2$ von zwei fremden Combinationen β_1, β_2 dar, so wird

$$(\alpha, 0) = \Pi(\alpha + \beta_1, \beta_2) \tag{2}$$

und alle Factoren $(\alpha + \beta_1, \beta_2)$ sind offenbar Kerne, weil $(\alpha + \beta_1) + \beta_2 = \alpha + \beta = \nu$ ist, wo ν wieder die aus allen n Elementen $1, 2 \ldots n$ bestehende Combination bedeutet; der Zerlegung $\beta_1 = 0$, $\beta_2 = \beta$ entspricht der Kern (α, β), und ebenso wird der Kern $(\nu, 0)$ durch die Zerlegung $\beta_1 = \beta$, $\beta_2 = 0$ erzeugt.

Unter einem *vollständigen Product* $\mathfrak{p}$ verstehe ich nun jedes Product aus lauter verschiedenen[1]) Kernen $\mathfrak{k}$, welches folgende Eigenschaft besitzt: wenn unter den Factoren $\mathfrak{k}$ sich der Kern (α, β) befindet, so enthält $\mathfrak{p}$ auch alle anderen Kernfactoren $(\alpha + \beta_1, \beta_2)$ des Elementes $(\alpha, 0)$ in (2). Unser Ziel besteht darin, zu beweisen, dass die oben genannte Dualgruppe $\mathfrak{P}$ nichts Anderes ist als der Inbegriff aller dieser vollständigen Producte $\mathfrak{p}$. Hierzu führen die folgenden Betrachtungen.

[1]) Dies Wort ist hier und im Folgenden immer nur im Sinne der äufserlichen Bezeichnung aufzufassen; es kann sehr wohl geschehen, dass in bestimmten Beispielen zwei äufserlich verschiedene Elemente einander gleich werden.

Zunächst überzeugt man sich leicht, dass das Product $(\alpha, 0)$ in (2) selbst die genannte Eigenschaft besitzt; denn wenn man aus seinen Factoren $\mathfrak{k}$ einen bestimmten Kern $(\alpha + \beta_1, \beta_2)$ herausgreift und die Combination β_2 auf alle Arten als Summe $\beta_3 + \beta_4$ von zwei fremden Combinationen β_3, β_4 darstellt, so erhält man

$$(\alpha + \beta_1, 0) = \Pi(\alpha + \beta_1 + \beta_3, \beta_4);$$

offenbar befinden sich aber alle Factoren dieses Productes auch unter den Factoren $\mathfrak{k}$ des Productes (2), und folglich ist $(\alpha, 0)$ wirklich ein vollständiges Product.

Aber diese Elemente $(\alpha, 0)$ sind keineswegs die einzigen vollständigen Producte; wählen wir z. B. $n = 4$ und betrachten das aus sechs verschiedenen Kernen (α, β) gebildete Product

$$\mathfrak{p} = (1234,0)(123,4)(124,3)(134,2)(12,34)(13,24),$$

so erhält man nach (2) für die Elemente $(\alpha, 0)$ die Zerlegungen

$$\begin{aligned}(1234,0) &= (1234,0)\\ (123,0) &= (1234,0)(123,4)\\ (124,0) &= (1234,0)(124,3)\\ (134,0) &= (1234,0)(134,2)\\ (12,0) &= (1234,0)(123,4)(124,3)(12,34)\\ (13,0) &= (1234,0)(123,4)(134,2)(13,24)\end{aligned}$$

und da alle rechts auftretenden Kerne auch Factoren des Productes $\mathfrak{p}$ sind, so ist letzteres vollständig, während z. B. das Product

$$(1234,0)(134,2)(12,34)$$

unvollständig ist, weil unter seinen Factoren die beiden, in (12,0) enthaltenen Kerne (123,4), (124,3) fehlen.

Die wichtigste Grundlage für unsere Untersuchung bildet aber der folgende

Satz I. Sind $\mathfrak{p}$, $\mathfrak{q}$ *vollständige Producte, so gilt dasselbe auch von* $\mathfrak{p} \pm \mathfrak{q}$, *und zwar ist* $\mathfrak{p} + \mathfrak{q}$ *das Product aller derjenigen verschiedenen Kerne, welche beiden Producten* $\mathfrak{p}$, $\mathfrak{q}$ *gemeinsam sind, und* $\mathfrak{p} - \mathfrak{q}$ *ist das Product aller verschiedenen Kernfactoren von* $\mathfrak{p}\mathfrak{q}$.

Beweis. Wir theilen die in den Producten $\mathfrak{p}$, $\mathfrak{q}$ auftretenden Kerne in drei Arten ein, in solche (η, ϑ), welche beiden gemeinsam sind, ferner in solche (α, β), welche nur in $\mathfrak{p}$, nicht in $\mathfrak{q}$ auftreten, endlich in solche (γ, δ), welche nur in $\mathfrak{q}$, nicht in $\mathfrak{p}$ auftreten; setzen wir zur Abkürzung die drei entsprechenden Producte

$$\Pi(\eta, \vartheta) = \mathfrak{r}, \quad \Pi(\alpha, \beta) = \mathfrak{m}, \quad \Pi(\gamma, \delta) = \mathfrak{n},$$

so wird

$$\mathfrak{p} = \mathfrak{r}\mathfrak{m}, \quad \mathfrak{q} = \mathfrak{r}\mathfrak{n}.$$

Wir vergleichen zunächst jeden Factor (α, β) von $\mathfrak{m}$ mit jedem Factor (γ, δ) von $\mathfrak{n}$ und setzen $\beta - \gamma = \varrho$, $\alpha - \delta = \sigma$. Macht man nun die Annahme, es sei $\sigma = 0$, so folgt aus dem in §. 3, S. 10 bewiesenen Satze, dass $\beta = \varrho + \delta$, $\gamma = \alpha + \varrho$ ist; mithin ist $(\gamma, \delta) = (\alpha + \varrho, \delta)$

ein Kernfactor von $(\alpha, 0)$, er muss daher, weil (α, β) ein Factor des vollständigen Productes $\mathfrak{p}$ ist, ebenfalls Factor von $\mathfrak{p}$ sein; dies widerspricht aber der obigen Definition von (γ, δ), und folglich ist unsere obige Annahme $\sigma = 0$ unzulässig. Da aus denselben Gründen auch der Durchschnitt $\varrho = \beta - \gamma$ von 0 verschieden, und ausserdem $\alpha + \beta = \gamma + \delta = \nu$ ist, so folgt (nach Satz III in §. 7), dass jeder Factor (α, β) von $\mathfrak{m}$ *fremd* zu jedem Factor (γ, δ) von $\mathfrak{n}$, mithin auch

$$\mathfrak{m} + \mathfrak{n} = \mathfrak{o}, \quad \mathfrak{p} + \mathfrak{q} = \mathfrak{r}(\mathfrak{m} + \mathfrak{n}) = \mathfrak{r}$$

ist. Betrachtet man nun irgend einen Factor (η, ϑ) von $\mathfrak{r}$ und zerlegt $(\eta, 0)$ in seine Kernfactoren nach (2), so muss jeder solche Factor, weil (η, ϑ) den beiden vollständigen Producten $\mathfrak{p}$, $\mathfrak{q}$ gemeinsam ist, ebenfalls gemeinsamer Factor von $\mathfrak{p}$, $\mathfrak{q}$, also auch Factor von $\mathfrak{r}$ sein, und folglich ist $\mathfrak{r}$ ein *vollständiges* Product, womit die Behauptungen des Satzes über $\mathfrak{p} + \mathfrak{q}$ erwiesen sind. Der andere Theil des Satzes ergiebt sich leicht aus

$$\mathfrak{p} - \mathfrak{q} = \frac{\mathfrak{p}\mathfrak{q}}{\mathfrak{p} + \mathfrak{q}} = \mathfrak{r}\mathfrak{m}\mathfrak{n} = \mathfrak{p}\mathfrak{n} = \mathfrak{q}\mathfrak{m};$$

denn jeder Factor (λ, μ) dieses Productes $\mathfrak{r}\mathfrak{m}\mathfrak{n}$ ist entweder in $\mathfrak{p}$ oder in $\mathfrak{q}$ enthalten, mithin ist auch jeder Kernfactor von $(\lambda, 0)$ ebenfalls Factor von $\mathfrak{p}$ oder $\mathfrak{q}$, also gewiss Factor von $\mathfrak{p} - \mathfrak{q}$, und da auch alle Factoren (λ, μ) verschieden sind, so ist auch $\mathfrak{p} - \mathfrak{q}$ ein *vollständiges* Product, w. z. b. w.

Durch wiederholte Anwendung dieses Satzes ergiebt sich ohne Weiteres, dass er auch für beliebig viele vollständige Producte $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3 \ldots$ gilt; sowohl ihr grösster gemeinsamer Theiler $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 + \cdots$, wie ihr kleinstes gemeinsames Vielfaches $\mathfrak{p}_1 - \mathfrak{p}_2 - \mathfrak{p}_3 - \cdots$ sind wieder vollständige Producte; der erstere ist das Product aller derjenigen verschiedenen Kerne, welche allen Producten $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3 \ldots$ gemeinsam sind, und das letztere ist das Product aller verschiedenen, in dem Producte $\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \ldots$ auftretenden Kerne. Hieraus ergiebt sich sofort der

Satz II. Jedes vollständige Product $\mathfrak{p}$ *von Kernen* (α, β) *ist das kleinste gemeinsame Vielfache aller ihnen entsprechenden Elemente* $(\alpha, 0)$.

Beweis. Jedes Element $(\alpha, 0)$ ist, wie schon oben bemerkt, ein vollständiges Product (2), mithin ist ihr kleinstes gemeinsames Vielfaches $\mathfrak{a}$ (nach der eben bewiesenen Regel) das Product aller in dem Producte $\Pi(\alpha, 0)$ auftretenden verschiedenen Kerne $\mathfrak{k}$; alle diese Kerne $\mathfrak{k}$ müssen aber auch in $\mathfrak{p}$ auftreten, weil $\mathfrak{p}$ als vollständiges Product zugleich mit (α, β) auch alle Kernfactoren $\mathfrak{k}$ von $(\alpha, 0)$ zu Factoren hat. Da umgekehrt jeder in $\mathfrak{p}$ auftretende Kern (α, β) auch ein Factor des Elementes $(\alpha, 0)$, also einer der Kerne $\mathfrak{k}$ ist, und da alle diese Kerne (α, β) auch verschieden sind, so folgt $\mathfrak{p} = \mathfrak{a}$, w. z. b. w.

Wir kehren nun zu der Dualgruppe $\mathfrak{P}$ zurück, welche aus den gegebenen n Elementen (1) durch wiederholte Anwendung der beiden Operationen $\pm$ entstehen soll. Durch die Operation $+$ werden zunächst alle Elemente von der Form $(\alpha, 0)$ erzeugt, und diese sind, wie oben bemerkt, lauter vollständige Producte; wendet man sodann auf beliebig viele Elemente $(\alpha, 0)$ des so erzeugten Systems die Operation $-$ an, so erhält man (nach Satz I) immer wieder vollständige Producte, und zwar entstehen auf diese Weise (nach Satz II) *alle* vollständigen Producte; endlich leuchtet ein, dass hiermit die Bildung des Systems $\mathfrak{P}$ schon vollendet ist, weil der Inbegriff aller vollständigen Producte (nach Satz I) die charakteristischen Eigenschaften einer *Dualgruppe* besitzt [1]).

Die Anzahl der in dieser Gruppe $\mathfrak{P}$ enthaltenen Elemente scheint mit der Anzahl n der gegebenen Elemente (1) sehr rasch zu wachsen; sie ist $= 18$ im Falle $n = 3$, und (wenn ich nicht irre) $= 166$ im Falle $n = 4$; einen allgemeinen Ausdruck für diese Anzahl zu finden, habe ich noch nicht versucht. Dagegen leuchtet ein, dass die Elemente von $\mathfrak{P}$, d. h. die vollständigen Producte $\mathfrak{p}$ sich nach der Anzahl der in ihnen auftretenden Kerne in $(2^n - 1)$ Stufen vertheilen, und dass jede folgende Stufe die *nächsten* Vielfachen von den Elementen der vorhergehenden Stufe enthält. Endlich will ich bemerken, dass diejenigen Elemente von $\mathfrak{P}$, welche auf *symmetrische* Weise aus den Elementen (1) gebildet sind, in einfachen Beziehungen zu den *symmetrischen Functionen* stehen, welche aus den Elementen (1) auf dieselbe Weise wie in der Algebra zusammengesetzt sind [2]); doch kann ich auf die Darstellung dieser Beziehungen hier nicht mehr eingehen.

---

[1]) Vergl. D., §. 169, S. 499, Anmerkung. — Die daselbst erwähnte, aus drei *Moduln* erzeugte Dualgruppe von 28 Moduln, welche den Idealtypus nicht besitzt, erfordert zu ihrer Bildung eine mehrmals abwechselnde Anwendung der beiden Operationen.

[2]) Vergl. D., §. 170, S. 503, Anmerkung.